US006636894B1

(12) **United States Patent**
Short et al.

(10) **Patent No.: US 6,636,894 B1**
(45) **Date of Patent: Oct. 21, 2003**

(54) **SYSTEMS AND METHODS FOR REDIRECTING USERS HAVING TRANSPARENT COMPUTER ACCESS TO A NETWORK USING A GATEWAY DEVICE HAVING REDIRECTION CAPABILITY**

(75) Inventors: **Joel E. Short**, Los Angeles, CA (US); **Frederic Delley**, Redwood City, CA (US); **Mark F. Logan**, Santa Monica, CA (US); **Florence C. I. Pagan**, Los Angeles, CA (US)

(73) Assignee: **Nomadix, Inc.**, Westlake Village, CA (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

(21) Appl. No.: **09/458,569**

(22) Filed: **Dec. 8, 1999**

Related U.S. Application Data

(60) Provisional application No. 60/111,497, filed on Dec. 8, 1998.

(51) **Int. Cl.**[7] **G06F 15/173**

(52) **U.S. Cl.** **709/225**; 709/249

(58) **Field of Search** 709/225, 226, 709/227, 229, 249; 707/1; 713/200, 201

(56) **References Cited**

U.S. PATENT DOCUMENTS

5,696,898	A *	12/1997	Baker et al.	713/201
5,761,683	A	6/1998	Logan et al.	
5,845,070	A *	12/1998	Ikudome	713/201
5,968,176	A	10/1999	Nessett et al.	
5,991,292	A *	11/1999	Focsaneanu et al.	370/352
6,219,694	B1 *	4/2001	Lazaridis et al.	709/206
6,317,790	B1 *	11/2001	Bowker et al.	709/225
6,317,837	B1 *	11/2001	Kenworthy	713/200
6,393,468	B1 *	5/2002	McGee	709/218
6,490,620	B1 *	12/2002	Ditmer et al.	709/224

FOREIGN PATENT DOCUMENTS

EP	0848338 A1	6/1998

(List continued on next page.)

OTHER PUBLICATIONS

Cisco; *Single–User Network Access Security TACACS+*; Mar. 30, 1995; 9 pages; *Cisco White Paper*; XP002124521.
D. Brent Chapman, Elizabeth D. Zwicky; *Building Internet Firewalls*, Nov. 1995; pp. 131–188; O'Reilly; XP002202789.

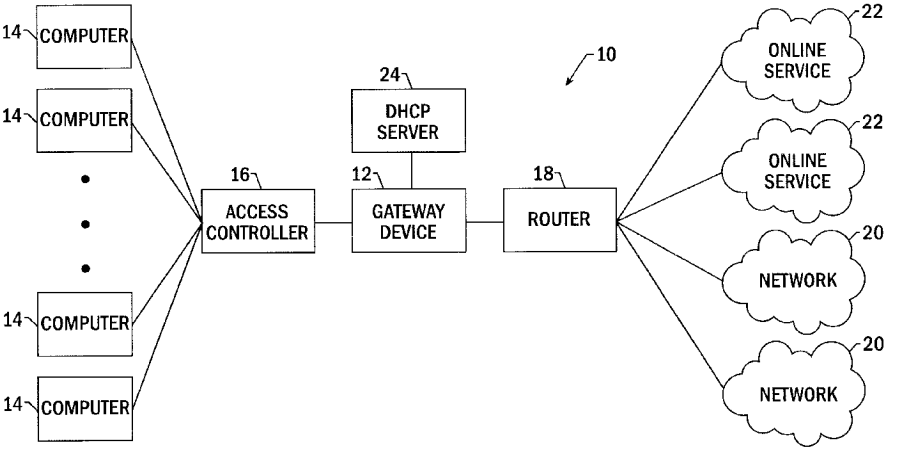
(List continued on next page.)

Primary Examiner—Mehmet B. Geckil
(74) *Attorney, Agent, or Firm*—Alston & Bird LLP

(57) **ABSTRACT**

Systems and methods for dynamically creating new users having transparent computer access to a destination network, wherein the users otherwise have access to a home network through home network settings resident on the users' computers, and wherein the users can access the destination network without altering the home network settings. The system includes a gateway device for receiving a request from a user for access to the destination network, a user profile database comprising stored access information and in communication with the gateway device, and an Authentication, Authorization and Accounting (AAA) server in communication with the gateway device and user profile database. The AAA server determines if user is entitled to access the destination network based upon the access information stored within the user profile database, and wherein the AAA server redirects the user to a login page where the access information does not indicate the user's right to access the destination network. The systems and methods of the present invention can also redirect users having transparent computer access to a destination network, wherein the users otherwise have access to a home network through home network settings resident on the users' computers, and wherein the users can access the destination network without altering the home network settings.

11 Claims, 1 Drawing Sheet



FOREIGN PATENT DOCUMENTS

EP	0889418 A2	1/1999
EP	0 909 073 A2	4/1999
EP	0986230 A2	3/2000
WO	WO 96/39668	12/1996
WO	WO 98/12643	3/1998
WO	WO 99/57865	11/1999
WO	WO 99/57866	11/1999
WO	WO 99/66400	12/1999

OTHER PUBLICATIONS

Susan Hinrichs; *Policy–Based Management Bridiging the Gap*; Dec. 6, 1999; pp. 209–218; Computer Security Applications Conference, 1999 (ACSAC 1999), Proceedings, 15th Annual Phoenix, Arizona, USA Dec. 6–10, 1999, Los Alamitos, California, IEEE Comput. Soc.; XP010368586.

* cited by examiner

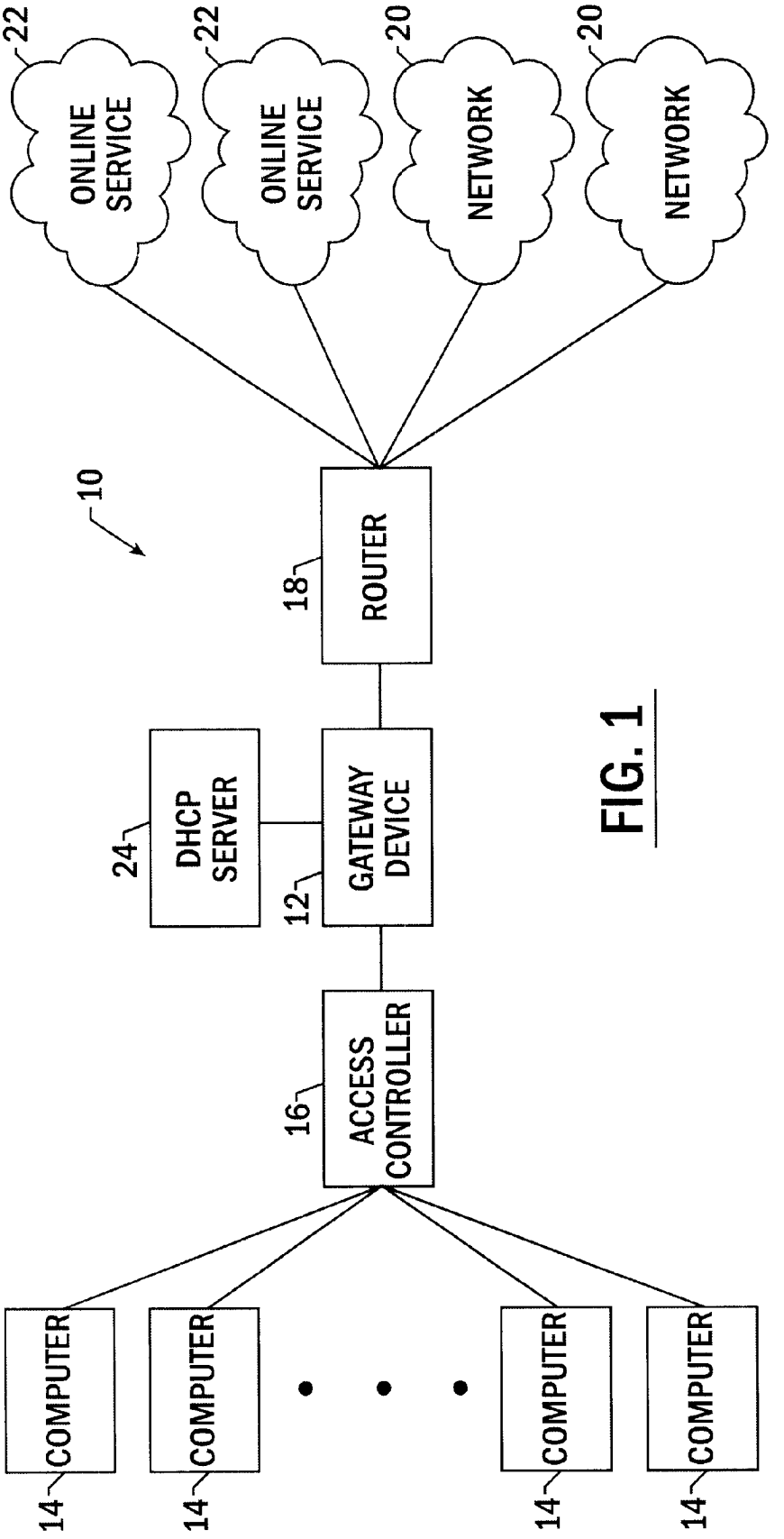

22
ONLINE SERVICE
22
ONLINE SERVICE
20
NETWORK
20
NETWORK
10
18
ROUTER
24
DHCP SERVER
12
GATEWAY DEVICE
16
ACCESS CONTROLLER
14
COMPUTER
14
COMPUTER
14
COMPUTER
14
COMPUTER

FIG. 1

SYSTEMS AND METHODS FOR REDIRECTING USERS HAVING TRANSPARENT COMPUTER ACCESS TO A NETWORK USING A GATEWAY DEVICE HAVING REDIRECTION CAPABILITY

CROSS-REFERENCE TO RELATED APPLICATIONS

The present application claim priority from U.S. Provisional Patent Application Ser. No. 60/111,497, filed Dec. 8, 1988 the contents of which are incorporated by reference.

FIELD OF THE INVENTION

The present invention relates generally to a gateway device and, more particularly, to a universal network gateway for redirecting to a portal page a computer transparently accessing a service provider network.

BACKGROUND OF THE INVENTION

In order for a computer to function properly in a network environment, the computer must be appropriately configured. Among other things, this configuration process establishes the protocol and other parameters by which the computer transmits and receives data. In one common example, a plurality of computers are networked to create a local area network (LAN). In the LAN, each computer must be appropriately configured in order to exchange data over the network. Since most networks are customized to meet a unique set of requirements, computers that are part of different networks are generally configured in different manners in order to appropriately communicate with their respective networks.

While desktop computers generally remain a part of the same network for a substantial period of time, laptops, handhelds, personal digital assistants (PDAs), cellphones or other portable computers (collectively "portable computers") are specifically designed to be transportable. As such, portable computers are connected to different networks at different times depending upon the location of the computer. In a common example in which the portable computer serves as an employee's desktop computer, the portable computer is configured to communicate with their employer's network, i.e., the enterprise network. When the employee travels, however, the portable computer may be connected to different networks that communicate in different manners. In this regard, the employee may connect the portable computer to the network maintained by an airport, a hotel, a cellular telephone network operator or any other locale in order to access the enterprise network, the Internet or some other on-line service. The portable computer is also commonly brought to the employee's residence where it is used to access various networks, such as, the enterprise network, a home network, the Internet and the like. Since these other networks are configured somewhat differently, however, the portable computer must also be reconfigured in order to properly communicate with these other networks. Typically, this configuration is performed by the user each time the portable computer is connected to a different network. As will be apparent, this repeated reconfiguration of the portable computer is not only quite time consuming, but is also prone to errors. The reconfiguration procedure may even be beyond the capabilities of many users or in violation of their employer's IT policy. Importantly, special software must also typically be loaded onto the user's computer to support reconfiguration.

As described by U.S. patent application Ser. No. 08/816,174 and U.S. Provisional Patent Application Nos. 60/111,497, 60/160,973, 60/161,189, 60/161,139, 60/160,890 and 60/161,182, a universal subscriber gateway device has been developed by Nomadix, Inc. of Westlake Village, Calif. The contents of these applications are incorporated herein by reference. The gateway device serves as an interface connecting the user to a number of networks or other online services. For example, the gateway device can serve as a gateway to the Internet, the enterprise network, or other networks and/or on-line services. In addition to serving as a gateway, the gateway device automatically adapts to a computer, in order that it may communicate with the new network in a manner that is transparent both to the user and the new network. Once the gateway device has appropriately adapted to the user's computer, the computer can appropriately communicate via the new network, such as the network at a hotel, at home, at an airport, or any other location, in order to access other networks, such as the enterprise network, or other online services, such as the Internet.

The portable computer user, and more specifically the remote or laptop user, benefits from being able to access a myriad of computer networks without having to undergo the time-consuming and all-too-often daunting task of reconfiguring their host computer in accordance with network specific configurations. In addition, no additional software need be loaded onto the computer prior to connection to the other network. From another perspective, the network service provider benefits from avoiding "on-site" visits and/or technical support calls from the user who is unable to properly re-configure the portable computer. In this fashion, the gateway device is capable of providing more efficient network access and network maintenance to the user and the network operator.

Gateway devices are typically used to provide network access to the remote portable computer user, such as users in hotels, airports and other location where the remote portable computer user may reside. Additionally, gateway devices have found wide-spread use in multi-resident dwellings as a means of providing the residents an intranet that networks the residents, broadband Internet access and the capability to adapt to the variances of the resident's individual enterprise network needs. With the advent of even smaller portable computing devices, such as handhelds, PDAs, and the like, the locations where these users may reside become almost limitless.

Through gateway devices Internet Service Providers (ISPs) or enterprise network (such as a LAN established by an entity such as a hotel) providers can permit a wide variety of users simple and transparent access to their networks and to other online services. To take advantage of transparent user access to their computer networks and online services enterprise networks or ISPs should be able to redirect users to portal pages that the enterprise or internet service providers wish the user to access or view. For instance, where users are located at an airport, the enterprise network administrator may wish to direct users to a portal page containing arrival and departure information, or to a portal page having the user's itinerary thereon to provide the user an incentive to access the network. ISPs, for example, may wish users to access the ISPs portal page for up to the date news and weather, information regarding the user's Internet service, and paid advertisements.

Homepage redirection has been accomplished in the prior art. For example, America Online (AOL) users, upon accessing the internet, are directed to an AOL homepage from which the users can select a variety of AOL services, and which includes advertising from various companies. Typically, direction of users to such a page benefits the ISP

because advertisers pay money to the ISP each time a user accesses the Internet, as subscribers are a captive audience to advertising. Advertisers pay for such advertising not only because of the captive audience, but because advertisers can tailor advertisements based upon the typical audience accessing the internet. Furthermore, AOL may market its services through its homepage, and its homepage may be attractive to potential subscribers. Directing users to a particular. page may serve an additional function. Users may be directed to a particular page, such as a login page, so that the user may enter login information to be authenticated and authorized access on the network. Furthermore, users may wish to establish their own specialized portal page, such as a page including favorite links, a page linking the user to the user's business, or a page including any other items relevant to the user.

However, such redirection of users to homepages has been traditionally based upon software installed on a user's computer and/or configurations of user computers in communication with a home network. For example, where a user's computer is appropriately configured for access to a home network, the user's computer can be configured to access a particular homepage on that network. This can be the case, for example, in businesses where users computers are configured to access an intranet homepage or an internet page specific to that company and located on the internet.

Therefore, a method and system would be desirable which enables a user transparent access to a computer network employing a gateway device where the computer network can provide access to users and direct the users to portal pages established by the user, network administrator or another entity, where the direction is preferably based upon attributes associated with a user, such as the user's location, identity, computer, or a combination thereof. Furthermore, such redirection should be able to redirect users to a login page when the user does not otherwise have access to online services or networks so that the user may login to be authenticated and authorized access on the network.

SUMMARY OF THE INVENTION

The present invention comprises a method and system for redirecting users to a portal page where users have transparent access to a computer network utilizing a gateway device. The method and system advantageously operates in a manner transparent to the user since the user need not reconfigure their computer and no additional software need be added to the computer for reconfiguration purposes.

According to the invention, users accessing the gateway device are redirected to a portal page. Where stored user profiles permit the users access to the destination network, the users can be forwarded to the destination network or a portal page established by the network, user, or another entity. Otherwise, users are directed to a login page in which the users must input user information so that the users can obtain access to networks and online services. The redirection function according to the present invention can be utilized to direct new or existing users to customized homepages established by the gateway device or individual users.

A method for dynamically creating new users having transparent computer access to a destination network is disclosed, wherein the users otherwise have access to a home network through home network settings resident on the users' computers, and wherein the users can access the destination network without altering the home network settings. The method includes receiving at a gateway device a request from a user for access to a destination network, determining if the user is entitled access to the destination network based upon a user profile corresponding to the user and stored within a user profile database in communication with the gateway device, and redirecting the user to a login page when the user profile does not include rights to access the destination network. Furthermore, the method of the present invention can include the step of forwarding the user to the destination network when the user profile includes rights to access the destination network. The method can also include the step of automatically redirecting the user to a portal page following receipt of a request for access to the destination network prior to determining if the user is entitled access to the destination network

According to one aspect of the invention, the method can include the step of establishing a login page on a webserver local to the gateway device prior to redirecting the user to the login page. The method can also include accepting user information at the login page which is thereafter utilized by the gateway device to authorize the user access to the destination network. The user profile database can be updated with the user information.

According to another aspect of the invention, the user may be forwarded from the login page and returned to a portal page or directed to a destination address which can be an Internet destination address. Redirecting the user to a login page can include redirecting a browser located on the user's computer to the login page. Furthermore, redirecting the browser located on the user's computer can include receiving a Hyper-Text Transfer Protocol (HTTP) request for the destination address and responding with an HTTP response corresponding to the login page.

According to another embodiment of the invention, a system for dynamically creating new users having transparent computer access to a destination network is disclosed, wherein the users otherwise have access to a home network through home network settings resident on the users' computers, and wherein the users can access the destination network without altering the home network settings. The system includes a gateway device for receiving a request from a user for access to the destination network, and a user profile database comprising stored access information and in communication with the gateway device. The system further includes an Authentication, Authorization and Accounting (AAA) server in communication with the gateway device and user profile database, where the AAA server determines if a user is entitled to access the destination network based upon the access information stored within the user profile database, and wherein the AAA server redirects the user to a login page where the access information does not indicate the user's right to access the destination network. The system can also direct the user to a portal page upon the user's access to the network, prior to determining the access rights of the user.

According to one aspect of the invention, the login page is maintained local to the gateway device. The user profile database and AAA server can also be located within the gateway device. Furthermore, the user profile database can be located within the AAA server.

According to another embodiment of the invention, the user profile database includes a plurality of user profiles, wherein each respective user profile of the plurality of user profiles contains access information. In addition, each respective user profile may contain historical data relating to the duration of destination network access for use in determining the charges due for the destination network access.

According to another embodiment of the invention, a method for redirecting users having transparent computer

access to a destination network is disclosed, wherein the users otherwise have access to a home network through home network settings resident on the users' computers, and wherein the users can access the destination network without altering the home network settings. The method includes receiving at a gateway device a request from a user for access to a destination address, such as an Internet address, and redirecting the user to a portal page, wherein the user computer remains configured for accessing the home network, and wherein no additional configuration software need be installed on the user's computer. Furthermore, redirecting the user to a portal page can comprise redirecting the user to a portal page created by an administrator associated with the portal page, or redirecting the user to a portal page customized by the user.

According to another embodiment of the invention, a system for redirecting users having transparent computer access to a destination network is disclosed, where the users otherwise have access to a home network through home network settings resident on the users' computers, and wherein the users can access the destination network without altering the home network settings. The system includes a gateway device for receiving a request from a user for access to the destination network, and an AAA server in communication with the gateway device, where the AAA server intercepts the request from the user for access to the destination network and redirects the user to a portal page, wherein the user's computer remains configured for accessing the home network, and wherein no additional configuration software need be installed on the user's computer. According to one aspect of the invention, the AAA server is located entirely within the gateway device. The portal page of the system can also be maintained on a server local to the gateway device.

A unique advantage of the transparent redirection of users to a portal page, and, in certain circumstances from the portal page, to a login page where users subscribe for network access is that a user can obtain access to networks or online services without installing any software onto the user's computer. On the contrary, the entire process is completely transparent to the user. As such, the method and apparatus of the present invention facilitates transparent access to destination networks without requiring a user to reconfigure the home network settings resident on the user computer and without having to install reconfiguration software.

The method and system of the various embodiments facilitate transparent access to a destination network. According to one embodiment, the method and system facilitate the addition of new subscribers to the network. According to another embodiment, all users can be redirected to a portal page, which can include advertising, without requiring reconfiguration of the users' computers, or new software to be added on the users' computers.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. **1** is a block diagram of a computer system that includes a gateway device for automatically configuring one or more computers to communicate via the gateway device with other networks or other online services, according to one embodiment of the present invention.

DETAILED DESCRIPTION OF ONE EMBODIMENT OF THE INVENTION

The present invention now will be described more fully hereinafter with reference to the accompanying drawings, in which preferred embodiments of the invention are shown. This invention may, however, be embodied in many different forms and should not be construed as limited to the embodiments set forth herein; rather, these embodiments are provided so that this disclosure will be thorough and complete, and will fully convey the scope of the invention to those skilled in the art. Like numbers refer to like elements throughout.

Referring now to FIG. **1**, a computer system **10** including a gateway device **12** is depicted in block diagram form. The computer system **10** typically includes a plurality of computers **14** that access a computer network in order to gain access to networks **20** or other online services **22**. For example, the computers **14** can be plugged into ports that are located in different rooms of a hotel, business, or a multi-dwelling unit. Alternatively, the computers **14** can be plugged into ports in an airport, an arena, or the like. The gateway device **12** provides an interface between the plurality of computers **14** and the various networks **20** or other online services **22**. One embodiment of a gateway device has been described by the aforementioned U.S. patent application Ser. No. 08/816,174.

Most commonly, the gateway device **12** is located near the computers **14** at a relatively low position in the overall network (i.e., the gateway device **12** will be located within the hotel, multi-unit residence, airport, etc.). However, the gateway device **12** can be located at a higher position in the system by being located closer to the various networks **20** or other online services **22**, if so desired. For example, the gateway device **12** could be located at a network operating center or could be located before or after a router **18** in the computer network. Although the gateway device **12** can be physically embodied in many different fashions, the gateway device **12** typically includes a controller and a memory device in which software is stored that defines the operational characteristics of the gateway device **12**. Alternatively, the gateway device **12** can be embedded within another network device, such as an access concentrator **16** or a router **18**. Moreover, the software that defines the functioning of the gateway device **12** can be stored on a PCMCIA card that can be inserted into a computer of the plurality of computers **14** in order to automatically reconfigure the computer to communicate with a different computer system, such as the networks **20** and online services **22**.

The computer system **10** typically includes an access concentrator **16** positioned between the computers **14** and the gateway device **12** for multiplexing the signals received from the plurality of computers onto a link to the gateway device **12**. Depending upon the medium by which the computers **14** are connected to the access concentrator, the access concentrator **16** can be configured in different manners. For example, the access concentrator can be a digital subscriber line access multiplexer (DSLAM) for signals transmitted via regular telephone lines, a cable head end for signals transmitted via coaxial cables, a wireless access point (WAP) for signals transmitted via a wireless network, a cable modem termination shelf (CMTS), a switch or the like. As also shown in FIG. **1**, the computer system **10** typically includes one or more routers **18** and/or servers (not shown in FIG. **1**) to control or direct traffic to and from a plurality of computer networks **20** or other online services **22**. While the computer system **10** is depicted to have a single router, the computer system **10** can have a plurality of routers, switches, bridges, or the like that are arranged in some hierarchical fashion in order to appropriately traffic to and from the various networks **20** or online services **22**. In

this regard, the gateway device **12** typically establishes a link with one or more routers. The routers, in turn, establish links with the servers of other networks or other online service providers, such as internet service providers, based upon the user's selection. It will be appreciated by one of ordinary skill in the art that one or more devices illustrated in FIG. **1** may be combinable. For example, although not shown, the router **18** may be located entirely within the gateway device **12**.

The gateway device **12** of the present invention is specifically designed to adapt to the configuration of each of the computers **14** that log onto the computer system **10** in a manner that is transparent to the user and the computer networks **20** or online services **22**. In the embodiment shown in FIG. **1**, the computer system **10** employs dynamic host configuration protocol (DHCP) service, which is a protocol well known to those of skill in the art and currently implemented in many computer networks. In DHCP networks an IP address is assigned to an individual computer of the plurality of computers **14** when the computer logs onto the computer network through communication with the gateway device **12**. The DHCP service can be provided by an external DHCP server **24** or it can be provided by an internal DHCP server located within the gateway device.

In order to allow a user of the computer to communicate transparently with computer networks **20** or online services **22**, the gateway device must be able to communicate with the user computer, as well as the various online services **22** or networks **20**. In order to support this communication, the gateway device **12** generally performs a packet translation function that is transparent to both the user and the network. In this regard, for outbound traffic from a computer to a network or on-line service, the gateway device **12** changes attributes within the packet coming from the user, such as the source address, checksum, and application specific parameters, to meet the criteria of the network to which the user has accessed. In addition, the outgoing packet includes an attribute that will direct all incoming packets from the accessed network to be routed through the gateway device. In contrast, the inbound traffic from the computer network or other online service that is routed through the gateway device undergoes a translation function at the gateway device so that the packets are properly formatted for the user's host computer. In this manner, the packet translation process that takes place at the gateway device **12** is transparent to the host, which appears to send and receive data directly from the accessed computer network. By implementing the gateway device as an interface between the user and the computer network or other online service, however, the user will eliminate the need to re-configure their computer **12** upon accessing subsequent networks as well as the need to load special configuration software on their computer to support the reconfiguration.

Communication between users and networks or online services may be effectuated through ports, for example, located within hotel rooms or multi-dwelling units, or through conventional dial-up communications, such as through the use of telephone or cable modems. According to one aspect of the invention, users can be are redirected to a portal page, as described below. After being redirected to the portal page, the user is subjected to a AAA process. Based upon the AAA process, the user may be permitted transparent access to the destination network or may be redirected to a login page in order to gather additional information to identify the user.

Identifying the user is crucial in authorizing access to networks or online services, as such services are typically provided for a fee and may be customized based upon the user, user's location, or user's computer. As discussed below, the user's identification may be used to direct the user to a specific portal page, which can be a particular webpage. As such, the system of the present invention includes means for identifying a user based upon an attribute associated with the user that is contained within the packet transmitted from the user's computer. Attributes can include any data well known in the art for identifying the user, the user's location, and/or the user's computer. In general, identifying a user's computer that accesses a network can be done by a media access control (MAC) associated with the computer. Identifying a computer based upon a MAC address is well known to those of skill in the art, and will not be discussed in detail herein. Additionally, the attribute can be based upon a user name, ID, or according to one advantageous embodiment described below, a particular location, such as from a communications port in a hotel room. As such, the location of the user can be the identifiable attribute.

According to one embodiment of the present invention, after a user accesses the computer network using a computer in communication with the gateway device **12**, as described above, the user is directed to a portal page. The portal page may be maintained by an ISP or an enterprise network, or by any entry maintaining a webpage on the Internet. According to one aspect of the invention, the portal page can be a webpage containing any information whatsoever, and can be created by the ISP, enterprise network administrator or user. The portal page can contain information specific to the user accessing the network, as discussed in detail below.

Regardless of whether a user accessing the computer network is authorized access to the network, the user is redirected to a portal page. After being redirected to a portal page, the gateway device of the present invention determines the authorization and access rights of the user based upon an Authentication, Authorization and Accounting method, as described in U.S. patent application Ser. No. 09/458602 entitled "Systems And Methods For Authorizing, Authenticating And Accounting Users Having Transparent Computer Access To A Network Using A Gateway Device" filed concurrently with this application and incorporated by reference.

According to one aspect of the invention, a user may be identified and authorized access to the network or online services based upon attributes associated with the user, such as the user's location or the user's computer. When this occurs, the user can be forwarded to a portal page unique to that user. As described below, and in the U.S. patent application incorporated by reference immediately above, the user may be identified without being queried to input any identification information so that upon accessing the computer network the user is automatically directed to a generic portal page or a portal page established specifically for and unique to that user. According to another aspect of the invention, a user may be identified and authorized access based upon the user's identity after being redirected to the portal page. The user may have to enter a login name and password while at the portal page or after being directed to a login page so that the ISP or other entity maintaining the gateway device can identify the user. After entering identifying data, the user may be directed to a particular portal page, as in the first aspect described above. According to a third aspect of the invention, the user is not authorized access to the network. Where this occurs the user will be directed from the portal page to a login page where the user will have to input identification information, such as the user's name, address, credit card number, and other relevant

data so that the user may be authorized to access the network. After the user enters sufficient login data to establish authorization, the user may be redirected to a portal page.

The redirection is accomplished by a Home Page Redirect (HPR) performed by the gateway device, a AAA server, or by a portal page redirect unit located internal to or external to the gateway device. To accomplish the redirection of a user to a portal page, HPR utilizes a Stack Address Translation (SAT) operation to direct the user to the portal page, which is preferably local to the gateway device so that the redirection will be efficient and fast. This is accomplished by redirecting the user to a protocol stack using network and port address translation to the portal server that can be internal to the computer network or gateway device. More specifically, the gateway device, AAA server or portal page redirect unit receives the user's HTTP request for a web page and sends back the HTTP response reversing the network and port address translation the portal server, essentially acting as a transparent 'go-between' to the user and portal server. It will be appreciated, however, that to receive the HTTP request the gateway device, AAA server or portal page redirect unit must initially open a Transmission Control Protocol (TCP) connection to a server in line with the user-requested internet address.

According to one aspect of the present invention, when a user initially attempts to access a destination location, the gateway device, AAA server or portal page redirect unit receives this request and routes the traffic to a protocol stack on a temporary server, which can be local to the gateway device. This can occur where a user initially opens a web browser resident on the user's computer and attempts to access a destination address, such as an Internet site. The destination address can also include any address accessible via the network or an online service, and can include the portal page. The protocol stack can pretend to be the user-entered destination location long enough to complete a connection or 'handshake'. Thereafter, this protocol stack directs the user to the portal server, which can be local to the gateway device to facilitate higher speed communication. The redirection to the portal server can be accomplished by redirecting web pages only, rather than all traffic, including E-mails, FTPs, or any other traffic. Therefore, once authorized, if a user does not attempt to access a webpage through the user's internet browser, the gateway device can forward the communication transparently to the user's requested destination without requiring the user to access the portal page. Furthermore, according to one aspect of the invention specific user-input destination addresses may be authorized to pass through the gateway device without being redirected.

The portal page can also be specialized based on the user, user's location, user's computer, or any combination thereof For example, assuming that the user has been authenticated and has authorization, the gateway device can present users with a portal page that identifies, among other things, the online services or other computer networks that are accessible via the gateway device. In addition, the portal page presented by the gateway device can provide information regarding the current parameters or settings that will govern the access provided to the particular user. As such, the gateway administrator can readily alter the parameters or other settings in order to tailor the service according to their particular application. Typically, changes in the parameters or other settings that will potentially utilize additional resources of the computer system will come at a cost, such that the gateway administrator will charge the user a higher rate for their service. For example, a user may elect to increase the transfer rate at which signals are transmitted across the computer network and pay a correspondingly higher price for the expedited service.

The portal page may include advertising tailored to the specific needs of the user. The gateway device would be capable of tailoring the material based upon user profiles in the network. The portal page may also incorporate surveys or links to surveys to provide the network provider with beneficial statistical data. As an ancillary benefit, the user who responds to the surveys may be rewarded with network access credit or upgraded quality. Additionally, the service provided could offer additional services to the user by way of the portal page or links to these services may be offered on the portal page. These services offered by the network service provider are not limited to the services related to the network connection. For example, a hotel may desire to offer the user in-room food service or a multi-unit dwelling may want to offer house cleaning service.

The portal page may also comprise information related to the status of the current network session. By way of example this information may include, current billing structure data, the category/level of service that the user has chosen, the bandwidth being provided to the user, the bytes of information currently sent or received, the current status of network connection(s) and the duration of the existing network connection(s). It is to be understood, by those skilled in the art to which this invention relates that all conceivable useful information relating to the current network session could be displayed to the user in a multitude of combinations as defined by the user and/or the gateway administrator. The gateway administrator will have the capability to dynamically change the information supplied in the portal page based on many factors, including the location of the user, the profile of the user and the chosen billing scheme and service level. The information provided in the portal page may prompt the user to adjust any number of specific parameters, such as the billing scheme, the routing, the level of service and/or other user-related parameters.

The portal page may be implemented with an object-oriented programming language such as Java developed by Sun Microsystems, Incorporated of Mountain View, Calif. The code that defines the portal page can be embodied within the gateway device, while the display monitor and the driver are located with the host computers that are in communication with the gateway device. The object oriented programming language that is used should be capable of creating executable content (i.e. self-running applications) that can be easily distributed through networking environments. The object oriented programming language should be capable of creating special programs, typically referred to as applets that can be incorporated in portal pages to make them interactive. In this invention the applets take the form of the portal pages. It should be noted that the chosen object-oriented programming language would require that a compatible web browser be implemented to interpret and run the portal page. It is also possible to implement the portal page using other programming languages, such as HTML, SGML and XML; however, these languages may not be able to provide all the dynamic capabilities that languages, such as Java provide.

By re-directing the user to the portal page the gateway administrator or network operator is provided the opportunity to present the user with updated information pertaining to the remote location (i.e. the hotel, the airport etc.). By way of example the portal page may provide for links to the corporate home page, a travel site on the Internet, an Internet

search engine and a network provider home page. Additionally, the buttons or any other field within the portal page may include other types of information options, such as advertising fields or user-specific links or fields based upon data found in the user's profile or inputted by the user.

It will be appreciated that the portal page is not limited to supplying information related to the user's billing and service plans. It is also possible to configure the portal page to include information that is customized to the user or the location/site from which the user is remotely located. For example, the user may be located at a hotel for the purpose of attending a specific convention or conference either in the hotel or within the immediate vicinity of the hotel. The gateway device may have "learned" this information about the user through an initial log-on profile inquiry or the gateway administer may have inputted this information into a database.

The gateway device can store user profile information within a user-specific AAA database, as described below, or it can store and retrieve data from external databases. The gateway device can be configured to recognize these profiles and to customize the portal page accordingly. In the hotel scenario, the portal page may include a link for convention or conference services offered by the hotel.

In another example of location specific portal page data, the user may be remotely accessing the gateway device while located in a specific airport terminal. The gateway device will be configured so that it is capable of providing ready access to information related to that specific airport terminal, i.e. information pertaining to the current flights scheduled to depart and arrive that terminal, the retail services offered in that specific terminal, etc. In this manner, the portal page may include a link for terminal specific flight information and/or terminal specific retail services available to the user.

It will also be appreciated that the HPR may be configured so a user is redirected to a portal page upon specific default occurrences, such as a time out, or according to preset time. For example, the portal page may act as a screen-saver, where the user is redirected to a portal page after a given period of inactivity. These functions may be established by the ISP or enterprise network administrator.

Customization of the information comprising the portal page is not limited to the gateway administrator or the network operator. The user may also be able to customize the information that is provided in the portal page. The user customization may be accomplished either directly by the user configuring the portal page manually or indirectly from the gateway device configuring the portal page in response to data found in the user-specific profile. In the manual embodiment the user may be asked to choose which information or type of information they would like supplied in the portal page for that specific network session. For instance, the user may require an alarm clock counter to insure an appointment is met or the user may require periodical updates of a specific stock quote. The information that a user customizes for the portal page may be network session specific, may be associated with the duration of a gateway subscription or may be stored in a user profile for an indefinite period of time. The gateway device's ability to communicate with numerous user databases provides the basis for storing user specific profiles for extended periods of time.

As explained above, the portal page presented to the user can be dependent upon an attribute associated with the user, such as the user's identification, the user's location, an address associated with the user's computer, or a combination thereof The means in which a user is identified and access rights are determined is based upon an Authentication, Authorization and Accounting (AAA) method implemented by the AAA server, and disclosed in U.S. patent application Ser. No. 09/458,602, and filed concurrently with this application.

One function of the AAA server is to identify the user in communication with the gateway device in a manner that is transparent to the user. That is, the user will not be required to reconfigure the computer or otherwise change the home network settings, and no additional configuration software will have to be added to the computer. According to one embodiment of the present invention, after a user is directed to a portal page, the AAA server can be accessed to authorize and authenticate the user. Therefore, upon accessing the network, the user may be forwarded to a generic portal page, and after the user may be authenticated, the user can be forwarded via HPR and SAT to a specialized portal page, as described above.

After receiving a request for access from a user, forwarding the user to a portal page, and identifying the user or location the AAA server then determines the access rights of the particular user. In addition to storing whether users have valid access rights, the user profile database can also include specialized access information particular to a specific location or user, such as the bandwidth of the user's access, or a portal page to which a user should be directed. For example, a user accessing the network from a penthouse may receive a higher access band rate than someone accessing the destination network from a typical hotel room. Additionally, a user profile can include historical data relating to a user's access to the network, including the amount of time a user has accessed the network. Such historical information can be used to determine any fees which may be charged to the user, or due from the user, for access. Specialized access information contained within the user profile may be established by the system administrator, or by the user who has purchased or otherwise established access to the network. For example, where a user is transparently accessing the gateway device from a hotel room, the hotel network administrator may enter user access information into the profile database based upon access rights associated with a room in the hotel. This can also be done automatically by the gateway device or a local management system, such as a hotel property management system, when the user checks into his or her room.

Assuming that a user does not have a subscription for access to the network, a login page enables new users to subscribe to the computer network so that they may subsequently obtain access to networks or online services transparently through the gateway device. The user may take steps to become authenticated so that the user's information may be recorded in the user profile database and the user is deemed valid. For example, a user may have to enter into a purchase agreement, requiring the user to enter a credit card number. If the user needs to purchase access, or if the system needs additional information about the user, the user is redirected from the portal page via HPR and SAT to a location, such as a login page, established to validate new users. SAT and HPR can intervene to direct the user to a webserver (external or internal) where the user has to login and identify themselves. Location-based information and authorization, as described in detail in U.S. patent application Ser. No. 60/161,093, incorporated herein by reference, can be sent to the portal page as part of this redirection process. This enables the portal page to be customized to

include customized information, such as locale restaurant ads or train schedules.

Assuming that a user has not been authorized access to the network based upon location based identification or user input identification, the user must provide the gateway device with sufficient information to become authorized access. Where the user is not authorized access the user is forwarded via HPR and SAT from the portal page to a login page. The login page enables new users to subscribe to the computer network so that they may subsequently obtain access to networks or online services transparently through the gateway device. To direct the users to a login page the AAA server calls upon the HPR function. The HPR directs the user to the login page, and after the user has entered requisite information into the login page, the AAA server adds the new information to the customer profile database and can direct the user to the user's desired destination, such as an Internet address or can return the user to a portal page, depending upon the design of the system. Thus, new users can gain access to networks or online services without being predefined in the user profile database.

After receiving the user's login information, the AAA server will create a user profile utilizing this information so that the user will be able to obtain immediate access to the network next time the user logs in without being required to enter login information again. The AAA server can create a profile for the user in a locally stored user profile database, or can update the user profile in a database external to the gateway device. Regardless of the location of the user profile, the next time the user attempts to login the user's profile will be located in the user profile database, the user's access rights determined, and the user allowed transparent access to networks or services.

Many modifications and other embodiments of the invention will come to mind to one skilled in the art to which this invention pertains having the benefit of the teachings presented in the foregoing descriptions and the associated drawings. Therefore, it is to be understood that the invention is not to be limited to the specific embodiments disclosed and that modifications and other embodiments are intended to be included within the scope of the appended claims. Although specific terms are employed herein, they are used in a generic and descriptive sense only and not for purposes of limitation.

That which is claimed:

1. A method for redirecting an original destination address access request to a redirected destination address, the method comprising the steps of:

receiving, at a gateway device, all original destination address access requests originating from a computer;

determining, at the gateway device, which of the original destination address requests require redirection;

storing the original destination address if redirection is required;

modifying, at the gateway device, the original destination address access request and communicating the modified request to a redirection server if redirection is required;

responding, at the redirection server, to the modified request with a browser redirect message that reassigns the modified request to an administrator-specified, redirected destination address;

intercepting, at the gateway device, the browser redirect message and modifying it with the stored original destination address; and

sending the modified browser redirect message to the computer, which automatically redirects the computer to the redirected destination address.

2. The method of claim **1**, further comprising the step of directing the computer to the stored original destination address after the computer has been automatically redirected to the redirected destination address.

3. The method of claim **2**, wherein the step of directing the computer to the stored original destination address occurs after a predetermined length of time.

4. The method of claim **2**, wherein the step of directing the computer to the stored original destination address occurs after a predetermined computer input event has occurred.

5. The method of claim **1**, wherein the step of responding, at the redirection server, to the modified request with a browser redirect message that reassigns the modified request to an administrator-specified, redirected destination address further comprises responding, at the redirection server, to the modified request with a browser redirect message that reassigns the modified request to a redirected destination address associated with a login page.

6. A system for redirecting an original destination address access request to a redirected destination address, the system comprising:

a computer that initiates original destination address requests;

a gateway device in communication with the computer, that receives the original destination address requests from the computer, determines if redirection of any of the original destination address requests is required, stores the original destination address request if redirection is required and modifies the original destination address request if redirection is required, and

a redirection server in communication with the gateway device that receives the modified request from the gateway device and responds with a browser redirect message that reassigns the request to an administrator-specified, redirect destination address,

wherein the gateway device intercepts the browser redirect message and modifies the response with the stored original destination address before forwarding the browser redirect message to the computer and wherein the computer receives the modified browser redirect message and the computer is automatically redirected to the redirect destination address.

7. The system of claim **6**, further comprising a user profile database in communication with the gateway device that includes stored user-access information.

8. The system of claim **6**, further comprising an Authentication, Authorization and Accounting (AAA) server in communication with the gateway device and user profile database, the AAA server determines if a user of the computer is entitled to access the original destination address requests based upon the user-access information stored within the user profile database.

9. The system of claim **6**, wherein the redirection server is located within the gateway device.

10. The system of claim **7**, wherein the user-profile database is located within the gateway device.

11. The system of claim **8**, wherein the AAA server is located within the gateway device.

* * * * *

US006636894C1

(12) EX PARTE REEXAMINATION CERTIFICATE (5316th)

United States Patent
Short et al.

(10) **Number: US 6,636,894 C1**
(45) **Certificate Issued: Mar. 28, 2006**

(54) **SYSTEMS AND METHODS FOR REDIRECTING USERS HAVING TRANSPARENT COMPUTER ACCESS TO A NETWORK USING A GATEWAY DEVICE HAVING REDIRECTION CAPABILITY**

(75) Inventors: **Joel E. Short**, Los Angeles, CA (US); **Frederic Delley**, Redwood City, CA (US); **Mark F. Logan**, Santa Monica, CA (US); **Florence C. I. Pagan**, Los Angeles, CA (US)

(73) Assignee: **Nomadix, Inc.**, Westlake Village, CA (US)

Reexamination Request:
No. 90/007,220, Sep. 24, 2004

Reexamination Certificate for:
Patent No.: **6,636,894**
Issued: **Oct. 21, 2003**
Appl. No.: **09/458,569**
Filed: **Dec. 8, 1999**

Related U.S. Application Data

(60) Provisional application No. 60/111,497, filed on Dec. 8, 1998.

(51) **Int. Cl.**
G06F 15/173 (2006.01)

(52) **U.S. Cl.** **709/225**; 709/249; 709/226

(58) **Field of Classification Search** 709/217, 709/219, 202, 220, 223, 224, 226, 227, 229, 709/238
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

5,781,550	A		7/1998	Templin et al.
5,802,320	A		9/1998	Baehr et al.
5,948,061	A		9/1999	Merriman et al.
6,014,698	A		1/2000	Griffiths
6,052,725	A	*	4/2000	McCann et al. 709/223
6,098,172	A		8/2000	Coss et al.
6,119,162	A		9/2000	Li et al.
6,226,677	B1		5/2001	Slemmer

OTHER PUBLICATIONS

Complaint, Demand for Jury Trial; *IPE Networks, Inc.* vs. *Nomadix, Inc.*; Case No. 04 CV 1485 DMS (POR); 45 pages; Filed Jul. 23, 2004; United States District Court, Southern District of California.

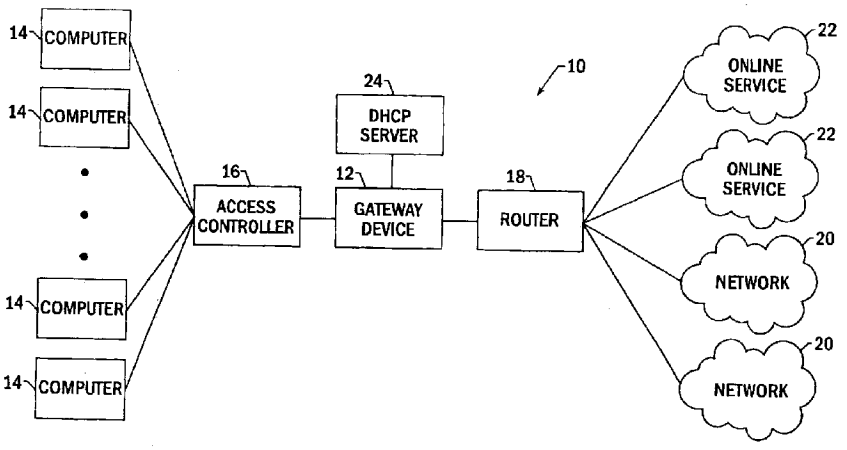
Amended Complaint, Demand for Jury Trial; *IPE Networks, Inc.* vs. *Nomadix, Inc.*; Case No. 04 CV 1485 DMS (POR); 48 pages; Sep. 20, 2004; United States District Court, Southern District of California.

(Continued)

Primary Examiner—Jeffrey Pwu

(57) **ABSTRACT**

Systems and methods for dynamically creating new users having transparent computer access to a destination network, wherein the users otherwise have access to a home network through home network settings resident on the users' computers, and wherein the users can access the destination network without altering the home network settings. The system includes a gateway device for receiving a request from a user for access to the destination network, a user profile database comprising stored access information and in communication with the gateway device, and an Authentication, Authorization and Accounting (AAA) server in communication with the gateway device and user profile database. The AAA server determines if user is entitled to access the destination network based upon the access information stored within the user profile database, and wherein the AAA server redirects the user to a login page where the access information does not indicate the user's right to access the destination network. The systems and methods of the present invention can also redirect users having transparent computer access to a destination network, wherein the users otherwise have access to a home network through home network settings resident on the users' computers, and wherein the users can access the destination network without altering the home network settings.



OTHER PUBLICATIONS

Answer and Counterclaims of Nomadix Inc. to the Amended Complaint; *IPE Networks, Inc.* vs. *Nomadix, Inc.*; Case No. 04 CV 1485 DMS (POR); 44 pages; Filed Oct. 21, 2004; United States District Court, Southern District of California.

Plaintiff/Counter–Defendant IPE Networks Inc.'s Reply to Defendant Nomadix, Inc.'s Counterclaim; *IPE Networks, Inc.* vs. *Nomadix, Inc.*; Case No. 04 CV 1485 DMS (POR); 8 pages; Nov. 15, 2004; United States District Court, Southern District of California.

David C. Plummer; *An Ethernet Address Resolution Protocol or Converting Network Protocol Addresses to 48.bit Ethernet Address for Transmission on Ethernet Hardware*; Nov. 1982; 8 pages; Network Working Group, Request for Comments 826.

Charles Hornig; *A Standard for the Transmission of IP Datagrams over Ethernet Networks*; Apr. 1984; 3 pages; Network Working Group, Request for Comments 894.

J. Postel; *Multi–Lan Address Resolution;* Oct. 1984; 14 pages; Network Working Group, Request for Comments 925.

R. Braden, J. Postel; *Requirements for Internet Gateways;* Jun. 1987; 50 pages; Network Working Group, Request for Comments 1009.

Smoot Carl–Mitchell, John S. Quarterman; *Using ARP to Implement Transparent Subnet Gateways*; Oct. 1987; 8 pages; Network Working Group, Request for Comments 1027.

P. Mockapetris; *Domain Names—Concepts and Facilities;* Nov. 1987; 49 pages; Network Working Group, Request for Comments 1034.

R. Droms; *Dynamic Host Configuration Protocol;* Oct. 1993; 35 pages; Network Working Group, Request for Comments 1531.

K. Egevang, P. Francis; *The IP Network Address Translator (NAT)*; May 1994; 9 pages; Network Working Group, Request for Comments 1631.

M. Chatel; *Classical Versus Transparent IP Proxies;* Mar. 1996; 32 pages; Network Working Group, Request for Comments 1919.

T. Berners–Lee, F. Fielding, H. Frystyk; *Hypertext Transfer Protocol—HTTP/1.0;* May 1996; 54 pages; Network Working Group, Request for Comments 1945.

Ari Loutonen, Kevin Altis; *World–Wide Web Proxies;* Apr. 1994; 8 pages.

John N. Stewart; *Working with Proxy Servers;* Mar. 1997; pp. 19–22; *WebServer Magazine.*

D. Wessels; *Squid Proxy Server Configuration File 1.93.2.2, "TAG deny_info";* Mar. 1997; 19 pages; available at <http://www.squid–cache.org/mail–archieve/squid–users/199703/att–0250/squid.conf>; (visited Feb. 1, 2005).

Cord Beerman; *Re: Support for cern like Pass/Fair proxy limits?;* 2 pages; available at <http://www.squid–cache.org/mail–archieve/squid–users/199611/0385.html> (visited Feb. 1, 2005).

Information Sciences Institute; *Internet Protocol, DARPA Internet Program, Protocol Specification;* Sep. 1981; 45 pages; available at <http://www.faqs.org/rfcs/rfc791.html> (visited 0002–01–2005).

Doug MacEachern; *Apache/Perl Integration Project;* README; 2 pages; available at <http://apache.perl.org>, <http://outside.organic.com/mail–archives/modperl>, and <http://www.ping.de/~fdc/mod_perl>.

Gisle Aas, Doug MacEachern; *Apache.pm;* 18 pages; available at <http://www.apache.org/docs>.

Mod_perl.c; Copyright; 1995–1997 The Apache Group; 20 pages.

* cited by examiner

EX PARTE REEXAMINATION CERTIFICATE ISSUED UNDER 35 U.S.C. 307

NO AMENDMENTS HAVE BEEN MADE TO THE PATENT

AS A RESULT OF REEXAMINATION, IT HAS BEEN DETERMINED THAT:

The patentability of claims **1**–**11** is confirmed.

* * * * *

US007194554B1

(12) **United States Patent**
Short et al.

(10) **Patent No.: US 7,194,554 B1**
(45) **Date of Patent: Mar. 20, 2007**

(54) **SYSTEMS AND METHODS FOR PROVIDING DYNAMIC NETWORK AUTHORIZATION AUTHENTICATION AND ACCOUNTING**

(75) Inventors: **Joel E. Short**, Los Angeles, CA (US); **Florence C. I. Pagan**, Los Angeles, CA (US); **Josh J. Goldstein**, Agoura Hills, CA (US)

(73) Assignee: **Nomadix, Inc.**, Westlake Village, CA (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 465 days.

(21) Appl. No.: **09/693,060**

(22) Filed: **Oct. 20, 2000**

Related U.S. Application Data

(63) Continuation-in-part of application No. 09/458,569, filed on Dec. 8, 1999, now Pat. No. 6,636,894.

(60) Provisional application No. 60/161,182, filed on Oct. 22, 1999, provisional application No. 60/160,890, filed on Oct. 22, 1999, provisional application No. 60/161,139, filed on Oct. 22, 1999, provisional application No. 60/161,189, filed on Oct. 22, 1999, provisional application No. 60/160,973, filed on Oct. 22, 1999, provisional application No. 60/161,181, filed on Oct. 22, 1999, provisional application No. 60/161,093, filed on Oct. 22, 1999, provisional application No. 60/111,497, filed on Dec. 8, 1998.

(51) **Int. Cl.**
G06F 15/16 (2006.01)

(52) **U.S. Cl.** **709/246**; 709/217; 709/220; 709/227; 709/230

(58) **Field of Classification Search** 709/229, 709/227, 225, 230, 217, 220, 246
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

5,113,499 A * 5/1992 Ankney et al. 340/5.74

(Continued)

FOREIGN PATENT DOCUMENTS

EP 0 762 707 A2 3/1997

(Continued)

OTHER PUBLICATIONS

USG Product Timeline, Nomadix, Inc., 2701 Ocean Park Blvd., Suite 231, Santa Monica, California 90405.

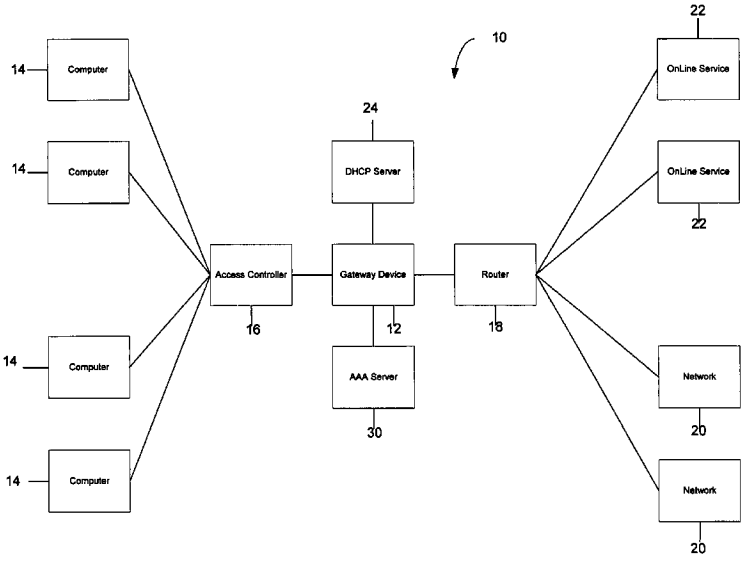
(Continued)

Primary Examiner—Saleh Najjar
Assistant Examiner—Michael Won
(74) *Attorney, Agent, or Firm*—Alston & Bird LLP

(57) **ABSTRACT**

Systems and methods for selectably controlling and customizing source access to a network, where the source is associated with a source computer, and wherein the source computer has transparent access to the network via a gateway device and no configuration software need be installed on the source computer to access the network. A user may be prevented access from a particular destination or site based upon the user's authorization while being permitted to access to other sites that the method and system deems accessible. The method and system can identify a source without that source's knowledge, and can access customizable access rights corresponding to that source in a source profile database. The source profile database can be a remote authentication dial-in user service (RADIUS) or a lightweight directory access protocol (LDAP) database. The method and system use source profiles within the source profile database to dynamically authorize source access to networks and destinations via networks.

24 Claims, 2 Drawing Sheets



U.S. PATENT DOCUMENTS

5,517,622	A *	5/1996	Ivanoff et al.	709/232
5,612,730	A	3/1997	Lewis	
5,623,601	A *	4/1997	Vu	713/201
5,742,668	A *	4/1998	Pepe et al.	455/415
5,864,610	A	1/1999	Ronen	
5,950,195	A	9/1999	Stockwell et al.	
5,968,176	A	10/1999	Nessett et al.	
6,130,892	A *	10/2000	Short et al.	370/401
6,161,139	A *	12/2000	Win et al.	709/225
6,226,752	B1 *	5/2001	Gupta et al.	713/201
6,317,790	B1 *	11/2001	Bowker et al.	709/225
6,385,653	B1 *	5/2002	Sitaraman et al.	709/230
6,502,131	B1 *	12/2002	Vaid et al.	709/224
6,598,167	B2 *	7/2003	Devine et al.	713/201
6,681,330	B2 *	1/2004	Bradford et al.	713/200
6,785,730	B1 *	8/2004	Taylor	709/230
6,856,676	B1 *	2/2005	Pirot et al.	379/201.01

FOREIGN PATENT DOCUMENTS

EP	0 909 073 A2	4/1999
WO	WO 98/16044	4/1998
WO	WO 99/57866	11/1999
WO	WO 99/66400	12/1999

OTHER PUBLICATIONS

Universal Subscriber Gateway, Nomadix, Inc., 2701 Ocean Park Blvd., Suite 231, Santa Monica, California 90405.

Schoen et al., *Convergence Between Public Switching and the Internet*, published Sep. 21, 1997 in *XVI World Telecom Congress Proceedings*, pp. 549-560.

Cisco; *Single-User Network Access Security TACACS+*; Mar. 30, 1995; 9 pages; *Cisco White Paper*; XP002124521.

D. Brent Chapman, Elizabeth D. Zwicky; *Building Internet Firewalls*; Nov. 1995; pp. 131-188; O'Reilly; XP002202789.

Susan Hinrichs; *Policy-Based Management Bridging the Gap*; Dec. 6, 1999; pp. 209-218; Computer Security Applications Conference, 1999 (ACSAC 1999), Proceedings, 15th Annual Phoenix, Arizona, USA Dec. 6-10, 1999, Los Alamitos, California; IEEE Comput. Soc.; XP010368586.

* cited by examiner

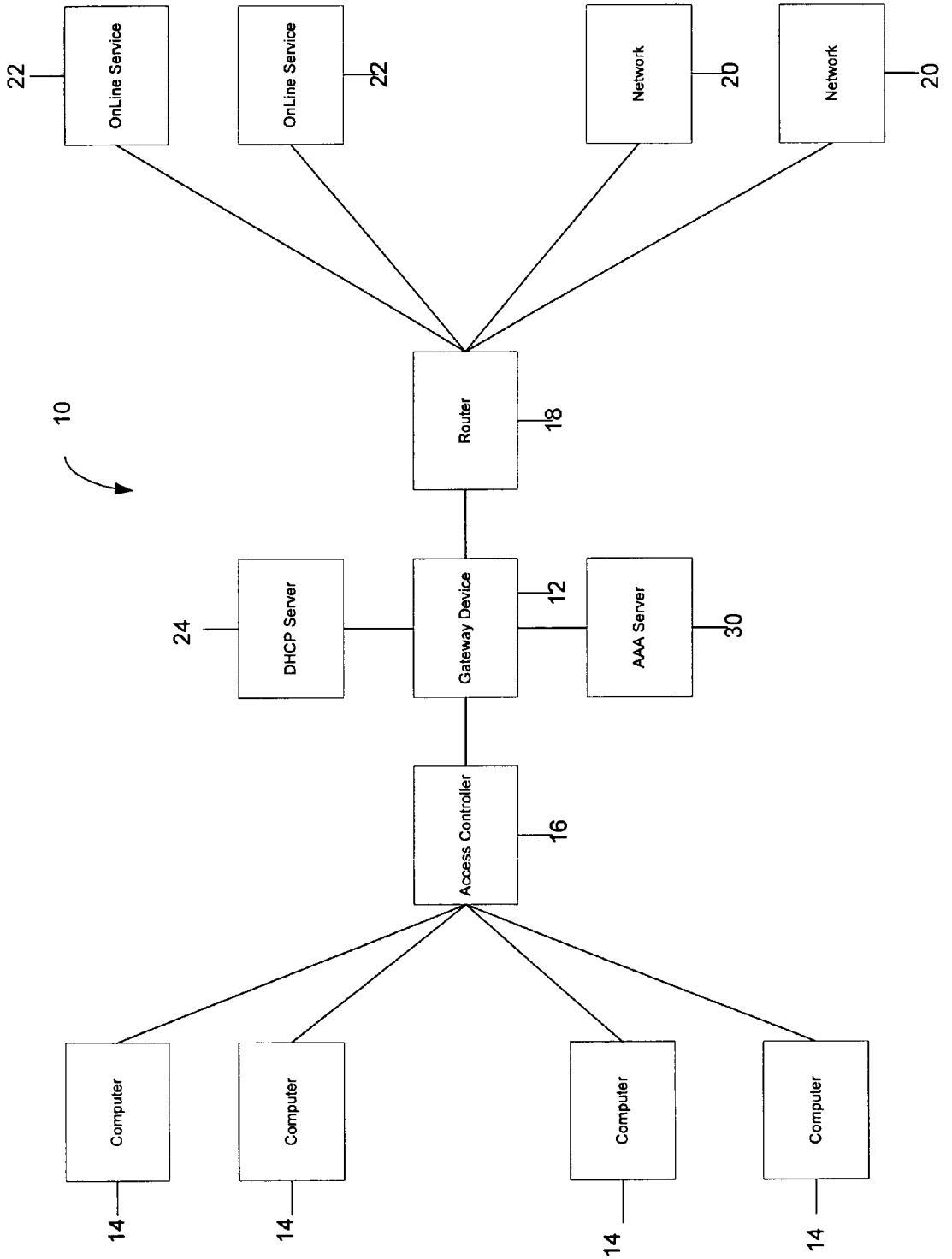

10
OnLine Service
22
OnLine Service
22
Network
20
Network
20
Router
18
Gateway Device
12
DHCP Server
24
AAA Server
30
Access Controller
16
Computer
14
Computer
14
Computer
14
Computer
14

FIG. 1

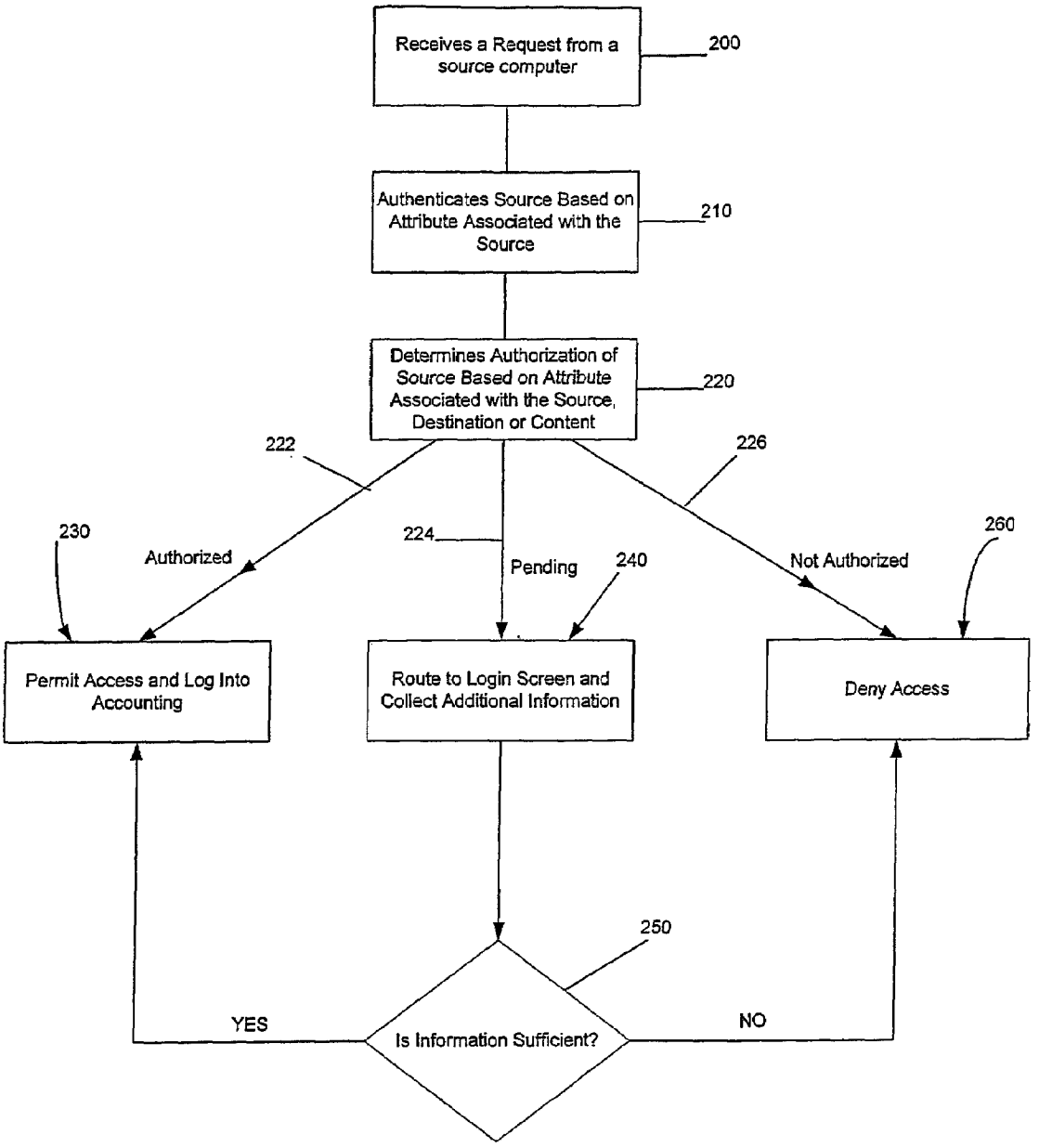

Receives a Request from a source computer
200
Authenticates Source Based on Attribute Associated with the Source
210
Determines Authorization of Source Based on Attribute Associated with the Source, Destination or Content
220
222
226
230
Authorized
224
Pending
240
Not Authorized
260
Permit Access and Log Into Accounting
Route to Login Screen and Collect Additional Information
Deny Access
250
YES
Is Information Sufficient?
NO

FIG. 2

SYSTEMS AND METHODS FOR PROVIDING DYNAMIC NETWORK AUTHORIZATION AUTHENTICATION AND ACCOUNTING

CROSS-REFERENCE TO RELATED APPLICATIONS

This application is a continuation-in-part of copending U.S. patent application Ser. No. 09/458,569, filed on Dec. 8, 1999, titled "Systems And Methods For Redirecting Users Having Transparent Computer Access To A Network Using A Gateway Device Having Redirection Capability", issued as U.S. Pat. No. 6,636,894, which claims the benefit of the filing date and priority to U.S. Provisional Application Ser. No. 60/111,497 filed on Dec. 8, 1998. This application also claims priority from U.S. application Ser. No. 09/458,602, filed Dec. 8, 1999, titled "Systems and Methods For Authorizing, Authenticating and Accounting Users Having Transparent Computer Access To A Network Using A Gateway Device," U.S. Provisional Application Ser. No. 60/161,182, filed Oct. 22, 1999, titled "Systems and Methods for Dynamic Bandwidth Management on a Per Subscriber Basis in a Computer Network," U.S. Provisional Application Ser. No. 60/160,890, filed Oct. 22, 1999, titled "Systems and Methods for Creating Subscriber Tunnels by a Gateway Device in a Computer Network," U.S. Provisional Application Ser. No. 60/161,139, filed Oct. 22, 1999, titled "Information And Control Console For Use With A Network Gateway Interface," U.S. Provisional Application Ser. No. 60/161,189, filed Oct. 22, 1999, titled "Systems and Methods for Transparent Computer Access and Communication with a Service Provider Network Using a Network Gateway Device," U.S. Provisional Application Ser. No. 60/160,973, filed Oct. 22, 1999, titled "Systems and Methods for Enabling Network Gateway Devices to Communicate with Management Systems to Facilitate Subscriber Management," U.S. Provisional Application Ser. No. 60/161,181, filed Oct. 22, 1999, titled "Gateway Device Having an XML Interface and Associated Method," and U.S. Provisional Application Ser. No. 60/161,093, filed Oct. 22, 1999, titled "Location-Based Identification and Authorization for use With a Gateway Device." All of the above applications are incorporated by reference in their entirety.

FIELD OF THE INVENTION

The present invention relates generally to systems and methods for controlling network access, and more particularly, to systems and methods for establishing dynamic user network access.

BACKGROUND OF THE INVENTION

User access to computer networks has traditionally been based upon a two step authentication process that either provides a user total network access, or refuses the user any access whatsoever. In the first step of the process, a user establishes a communication link with a network via a telephone line, dedicated network connection (e.g., Broadband, Digital Signal Line (DSL)), or the like. In the second step of the authentication process, the user must input identification information to gain access to the network. Typically, the input identification information includes a user name and password. Using this information, the network or service provider verifies that the user is entitled to access the network by determining whether the identification information matches subscriber information contained in a

subscriber table (or database) that stores identification information for all users authorized to access the network. Where user input information matches subscriber data in the subscriber table, the user is authorized to access any and all services on the network. On the other hand, if the user input identification information fails to match subscriber data in the table, the user will be denied access to the network. Thus, once a user's identity is compared to data stored within a subscription table, the user is either entitled network access, or denied access altogether. Furthermore, where the user is authorized access to the network, the user is typically authorized to access any destination accessible via the network. Therefore, conventional authentication of users is based on an all-or-nothing approach to network access.

In many conventional network access applications, such as in conventional Internet access applications, the subscriber database (or table) not only stores data corresponding to the identity of subscribers authorized to access the network, but also stores information that can vary based upon the particular subscriber. For instance, the subscriber database can include subscriber profiles that indicate the type of access a subscriber should receive, and other related information, such as the fees due by the subscriber for network access. Although information in the subscriber database may vary from user to user, information unique to the database is generally used for billing or network maintenance purposes. For instance, conventional subscriber databases typically include data such as the cost the subscriber is paying for network access, and the amount of time the subscriber has accessed the network. Thus, where a subscriber to an Internet Service Provider (ISP) has purchased Internet access, a source profile database may contain information that enables a user to be authenticated and tracks the user's access for accounting purposes, such as maintaining a log of the user's time on the network.

Additionally, in conventional network access systems, in order for a user to connect to on-line services (e.g., the Internet), the user must install client side software onto the user's computer. Client side software is typically provided by a network administrator or network access provider, such as an ISP with whom the user has subscribed for Internet access, and enables the client to configure his or her computer to communicate with that network access provider. Continuing with the illustrative example of a user accessing the Internet via an ISP, the user must install ISP software on the client computer, and thereafter establish an account with the ISP for Internet access. Typically, a user subscribes to an ISP, such as America Online™, Earthlink™, Compuserve™ or the like, by contracting directly with the ISP for Internet access. Usually, the user pays for such Internet access on a monthly fixed fee basis. Regardless of the user's location, the user may dial up an access number provided by the ISP and obtain Internet access. The connection is often achieved via a conventional telephone modem, cable modem, DSL connection, or the like.

Because users accessing networks through conventional methods, such as through ISPs, are either allowed or denied access to a network in an all or nothing approach, users cannot be dynamically authorized access to a network such that the user's access and authorization to particular networks or sites is customizable. What is needed is a method and system that allows users dynamic and customizable access that may vary based upon any number of variables associated with a user, such as a user location, user name or password, user computer, or other attributes. For example, it would be advantageous for some users to be authorized access to all Internet sites, while others may be denied

access to particular sites. In addition to authorizing user access to a network, it would be advantageous for a network, such as an ISP or enterprise network, to selectively permit users a range of authorization, such that the user's access is not based upon an all or nothing approach.

SUMMARY OF THE INVENTION

The present invention includes a method and system for selectively implementing and enforcing Authentication, Authorization and Accounting (AAA) of users accessing a network via a gateway device. According to the present invention, a user may first be authenticated to determine the identity of the user. The authentication capability of the system and method of the present invention can be based upon a user ID, computer, location, or one or more additional attributes identifying a source (e.g., a particular user, computer or location) requesting network access. Once authenticated, an authorization capability of the system and method of the present invention is customized based upon the identity of the source, such that sources have different access rights based upon their identity, and the content and/or destination requested. For instance, access rights permit a first source to access a particular Internet destination address, while refusing a second source access to that same address. In addition, the authorization capability of the system and method of the present invention can be based upon the other information contained in the data transmission, such as a destination port, Internet address, TCP port, network, or similar destination address. Moreover, the AAA of the present invention can be based upon the content type or protocol being transmitted. By authenticating users in this manner, each packet can be filtered through the selective AAA process, so that a user can be identified and authorized access to a particular destination. Thus, each time the user attempts to access a different destination, the user is subject to the AAA, so that the user may be prevented access from a particular site the AAA system and method deem inaccessible to the user based upon the user's authorization while permitting access to other sites that the AAA method and system deem accessible. Additionally, according to one embodiment of the invention, source access to the network may be tracked and logged by the present invention for accounting and historical purposes.

According to one embodiment of the invention, there is disclosed a method for selectably controlling and customizing source access to a network, wherein the source is associated with a source computer, and wherein the source computer has transparent access to the network via a gateway device and no configuration software need be installed on the source computer to access the network. The method includes receiving at the gateway device a request from the source computer for access to the network, identifying an attribute associated with the source based upon a packet transmitted from the source computer and received by the gateway device, and accessing a source profile corresponding to the source and stored in a source profile database, wherein the source profile is accessed based upon the attribute, and wherein the source profile database is located external to the gateway device and in communication with the gateway device. The method also includes determining the access rights of the source based upon the source profile, wherein access rights define the rights of the source to access the network.

According to one aspect of the invention, determining the access rights of the source based upon the source profile includes determining the access rights of the source based upon the source profile, wherein the access rights define the rights of the source to access a requested network destination. According to another aspect of the invention, the method includes assigning a location identifier to the location from which requests for access to the network are transmitted, and the location identifier is the attribute associated with the source. Furthermore, according to the invention, accessing a source profile corresponding to the source can include accessing a source profile stored in a source profile database, where the source profile database includes a remote authentication dial-in user service (RADIUS), or a lightweight directory access protocol (LDAP) database.

According to yet another aspect of the invention, the method includes updating the source profile database when a new source accesses the network. Additionally, the method can include maintaining in the source profile database a historical log of the source's access to the network. Moreover, the attribute associated with the source can be based upon a MAC address, User ID or VLAN ID associated with the source computer from which the request for access to the network was transmitted. According to yet another aspect of the invention, receiving at the gateway device a request from a source for access can include the step of receiving a destination address from the source.

According to another embodiment of the invention, there is disclosed a system for selectably controlling and customizing access, to a network, by a source, where the source is associated with a source computer, and wherein the source computer has transparent access to the network via a gateway device and no configuration software need be installed on the source computer to access the network. The system includes a gateway device for receiving a request from the source for access to the network, and a source profile database in communication with the gateway device and located external to the gateway device, wherein the source profile database stores access information identifiable by an attribute associated with the source, and wherein the attribute is identified based upon a data packet transmitted from the source computer and received by the gateway device. The system also includes a AAA server in communication with the gateway device and source profile database, wherein the AAA server determines if the source is entitled to access the network based upon the access information stored within the source profile database, and wherein the AAA server determines the access rights of the source with the access rights defining the rights of the source to access destination sites via the network.

According to one aspect of the invention, the packet received by the gateway device includes at least one of VLAN ID, a circuit ID, and a MAC address. Additionally, according to another aspect of the invention, the source profile database includes a remote authentication dial-in user service (RADIUS) or a lightweight directory access protocol (LDAP) database. Furthermore, the source profile database can include a plurality of source profiles, wherein each respective source profile of the plurality of source profiles contains access information. According to the invention, each respective source profile can also contain historical data relating to the duration of network access for use in determining the charges due for the network access. According to yet another aspect of the invention, the source profile database can be located within the AAA server.

According to another embodiment of the present invention, there is disclosed a method for redirecting a source attempting to access a destination through a gateway device, wherein source is associated with a source computer, and wherein the gateway device enables the source to commu-

nicate with a network without requiring the source computer to include network software configured for the network. The method includes receiving at the gateway device a request from the source to access the network, identifying the source based upon an attribute associated with the source, and accessing a source profile database located external to the gateway device, where the source profile database stores access rights of the source. The method further includes determining the access rights of the source based upon the identification of the source, wherein the access rights define the rights of the source to access destination sites via the network.

According to one aspect of the invention, accessing a source profile database includes accessing a source profile database that includes a remote authentication dial-in user service (RADIUS), or a lightweight directory access protocol (LDAP) database. According to another aspect of the invention, the method can include assigning a location identifier to the location from which requests for access to the network are transmitted, wherein the location identifier is the attribute associated with the source. The method can also include updating the source profile database when a new source accesses the network, and maintaining in an accounting database a historical log of the source's access to the network, wherein the accounting database is in communication with the source profile database.

According to yet another aspect of the invention, receiving at the gateway device a request from a source for access can include the step of receiving a destination address from the source. Moreover, determining if the source computer is entitled to access the destination address can further include denying the source computer access where the source profile indicates that the source computer is denied access. Determining if the source is entitled to access the network can also further include directing the source to a login page when the source profile is not located within the source profile database.

According to yet another embodiment of the invention, there is disclosed a system for enabling transparent communication between a computer and a service provider network. The system includes a computer, and a network gateway device in communication with the computer for connecting the computer to a computer network, where the network gateway device receives source data that represents a user attempting to access said computer network. The system also includes a service provider network in communication with the network gateway device, where the service provider network includes an authentication server located external to the network gateway device and in communication with the network gateway device. The authentication server has therein a source profile database comprising source profiles that represent users authorized to access said computer network, and compares the source data to said source profiles to determine if the user attempting to access the computer network can access the computer network.

According to one aspect of the invention, the system can include an accounting system for maintaining historical data concerning use of the service provider network. According to another aspect of the invention, the authentication server includes a remote authentication dial-in user service (RADIUS), or a lightweight directory access protocol (LDAP) database. Furthermore, the source profile database can include a plurality of source profiles, where each respective source profile of the plurality of source profiles contains access information. According to yet another aspect of the invention, the source data includes an attribute associated with the computer and transmitted from the computer to the gateway device. According to anther aspect of the invention, the source data includes login information associated with a respective user.

The Authentication, Authorization and Accounting method and system according to the present invention enable users transparent access to a computer network employing a gateway device. Therefore, each user may have differing rights to access services, sites or destinations via the network. Thus, the present invention differs from conventional AAA methods and systems by offering dynamic AAA services which authenticate users and offer those users varying degrees of authorization to utilize the accessed network. Furthermore, the source profile database of the present invention can be located external to the gateway device, and on a network non-local to the network from which access is requested. An external source profile database is desirable because each gateway device allows a finite number of users to access the network, so that multiple gateway devices may be required. Additionally, administering and maintaining one consolidated database of authentication data is easier than multiple smaller databases. Moreover, locating the database external to the local network allows an ISP or third party provider to maintain the confidentiality of the information stored within the database and maintain and control the database in any manner the third party provider so desires.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. **1** is a block diagram of a computer system that includes a AAA server for authenticating, authorizing and accounting sources accessing networks and/or online services, according to one embodiment of the present invention.

FIG. **2** is a flow chart of a method in which a AAA server performs authentication, authorization, and accounting, according to one aspect of the invention.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

The present invention now will be described more fully hereinafter with reference to the accompanying drawings, in which preferred embodiments of the invention are shown. This invention may, however, be embodied in many different forms and should not be construed as limited to the embodiments set forth herein; rather, these embodiments are provided so that this disclosure will be thorough and complete, and will fully convey the scope of the invention to those skilled in the art. Like numbers refer to like elements throughout.

Referring now to FIG. **1**, a computer system **10** is illustrated in block diagram form. The computer system **10** includes a plurality of computers **14** that can communicate with one or more online services **22** or networks via a gateway device **12** providing the interface between the computers **14** and the various networks **20** or online services **22**. One embodiment of such a gateway device has been described in U.S. patent application Ser. No. 08/816,174 (referred to herein as the Gateway Device Application), the contents of which are incorporated herein by reference. Briefly, the gateway device **12** facilitates transparent computer **14** access to the online services **22** or networks **22**, such that the computers **14** can access any networks via the device **12** regardless of their network configurations. Additionally, the gateway device **12** includes the ability to recognize computers attempting to access a network **12**, the

location of computers attempting to access a network, the identity of users attempting to gain network access, and additional attributes, as will be discussed below with respect to the dynamic AAA methods and systems of the present invention.

As illustrated in FIG. **1**, the computer system **10** also includes an access concentrator **16** positioned between the computers **14** and the gateway device **12** for multiplexing the signals received from the plurality of computers onto a link to the gateway device **12**. Depending upon the medium by which the computers **14** are connected to the access concentrator, the access concentrator **16** can be configured in different manners. For example, the access concentrator can be a digital subscriber line access multiplexer (DSLAM) for signals transmitted via regular telephone lines, a cable head end (a Cable Modem Termination Shelf (CMTS)) for signals transmitted via coaxial cables, a wireless access point (WAP) for signals transmitted via a wireless network, a switch, or the like.

The computer system **10** further includes a AAA server **30** that dynamically authenticates and authorizes user access, as explained in detail below, such that users are subjected to a AAA process upon attempting to gain access to a network through the gateway device **12**. Finally, as is shown in FIG. **1**, the computer system **10** typically includes one or more routers **18** and/or servers (not shown in FIG. **1**) to control or direct traffic to and from a plurality of computer networks **20** or other online services **22**. While the computer system **10** is depicted to have a single router, the computer system **10** can have a plurality of routers, switches, bridges, or the like that are arranged in some hierarchical fashion in order to appropriately route traffic to and from the various networks **20** or online services **22**. In this regard, the gateway device **12** typically establishes a link with one or more routers. The routers, in turn, establish links with the servers of the networks **20** or online services **22**, based upon the user's selection. It will be appreciated by one of ordinary skill in the art that one or more devices illustrated in FIG. **1** may be combinable. For example, although not shown, the router **18** may be located entirely within the gateway device **12**.

Users and computers attempting to access a network **20** or online service **22** via the gateway device **12** are referred to hereinafter as sources. According to AAA methods and systems of the present invention, a source attempting to access a network via the gateway device **12** is authenticated based on attributes associated therewith. These attributes can include the identity of a particular user or computer, location through which access is requested, requested network or destination, and the like. As is explained in detail in the Gateway Device Application, these attributes are identified by data packets transmitted to the gateway device **12** from the computers through which access is requested. According to one embodiment, methods and systems of the present invention provide dynamic authentication, authorization and accounting based upon these attributes. Generally, as used herein authentication refers to the identification of the source, authorization refers to the determination of permittable source access, and accounting refers to the tracking of a source's access to a network.

Referring now to the authentication function of systems and methods of present invention, it will be appreciated that authenticating a source attempting to access the network is often crucial to network administration, as network access and services are not typically laid open for all users regardless of identity or payment. As stated above, a source may be identified by the gateway device **12** by one or more attributes contained within data packets transmitted to the device from the computer associated with the source attempting to access a network or service, referred to hereinafter as the source computer. For instance, where the source is a user, the source computer is the computer through which the user is attempting to access a network or network destination. On the other hand, where the source is a computer through which one or more user may request access to a network, the source computer is that computer through which access is requested.

According to one aspect of the invention, a source computer attempting to access a network via the gateway device **12** may be identified one or more attributes that include a circuit ID, MAC address, user name, ID and/or password, or particular location (e.g., a communications port in a hotel room), or the like, transmitted to the gateway device **12** via data packets generated by the source computer, as described in U.S. Provisional Application Ser. No. 60/161,093, titled "Location-Based Identification and Authorization for use With a Gateway Device." It will be appreciated that one or more of these attributes can be used in the present invention to identify the source accessing the network. By means of an illustrative example, where sources are different users having dissimilar authentication and authorization rights, the users may identify themselves by their respective login information (e.g., user name and password) such that they will be independently identified despite the use of the same equipment, such as the same computer. On the other hand, where the source is a computer, diverse users using the computer will have like authentication and authorization rights regardless of the individual rights of each user, as the rights are associated with the computer (e.g., identified by MAC address), rather than with the respective users.

The authentication of sources via an attribute associated with the source is performed by the AAA server **30**, illustrated in FIG. **1**. The AAA server **30** stores source profiles corresponding to sources identified by the AAA server **30**. According to one aspect of the present invention, the AAA server **30** is located entirely within the gateway device **12**. According to another aspect of the invention, the AAA server **30** can comprise a plurality of components, at least some of which are external to the gateway device **12**, or alternatively, the AAA server **30** can be located entirely external to the gateway device **12**. For example, the location of the AAA server **30** may be such that the gateway device **12** communicates with the AAA server **30** via internet protocol.

According to one embodiment of the invention, the AAA server **30** can be maintained by an ISP, which identifies sources authorized to communicate with the network via the ISP. Therefore, it will be appreciated that the AAA server **30** may be located at any internet address and stored on any computer accessible via internet protocol.

According to one aspect of the invention, a separate source profile exists for each source accessing the system. Source profiles are maintained in a source profile database, which may be an internal component of the AAA server **30**, an external component of the AAA server **30**, or a separate component in communication with the AAA server **30**. Preferably, the source profile database is located external to the gateway device and network to alleviate administrative burden on the network so that the network does not have to set up and maintain separate authentication databases on each network or gateway device. This is also preferable because each gateway device **12** allows a finite number of users to access the network, which requires multiple gateway devices to accommodate a large number of sources. Secondly, administering and maintaining one consolidated

database of authentication data is easier than multiple smaller databases. Lastly, locating the source profile database external to the local network can allow an ISP or third party provider to maintain the confidentiality of the information stored within the database and maintain and control the database in any manner the third party provider so desires.

The source profile includes one or more names, passwords, addresses, VLAN tags, MAC addresses and other information pertinent to identify, and, if so desired, bill, a source. Upon a source's attempt to access a network via the gateway device **12**, the AAA server **30** attempts to authenticate the source by comparing stored source profiles in the source profile database with the attributes received from the gateway device **12** or source to determine the source identity. As an illustrative example, where a user attempts to access the network by entering a user ID and password, the user ID and password are compared against all IDs and passwords stored in the source profile database to determine the identity of the user. As such, the source profile database generally comprises a database or data storage means in communication with processing means located within the AAA server **30** or gateway device **12**, where the source profile database and processor work in conjunction to compare received attributes to stored source profile information, as is well known in the art.

The source profile database may comprise programmable storage hardware or like means located on a conventional personal computer, mainframe computer, or another suitable storage device known in the art. Additionally, the means for comparing the received data to the data within the database can comprise any software, such as an executable software program, which can compare data. For example, the AAA server **30** may store source profiles on a hard drive of a personal computer, and the means for comparing the received source data to the source profiles resident on the computer can include computer software, such as Microsoft Excel (Microsoft Excel is a trademark of Microsoft Corporation, Redmond, Wash.). According to another embodiment of the invention, the AAA server **30** or source profile database can comprise a Remote Authentication Dial-In User Service (RADIUS) or a Lightweight Directory Access Protocol (LDAP) database, which are well known to those of skill in the art.

If a source fails to correspond to a source profile in the AAA server **30** at the time of authentication, the source will not be permitted access to the network. When this occurs, a user or user associated with a non-user source may be requested to input source profile information to the AAA server **30** so that the AAA server **30** can add the source's profile to the AAA server **30**, and more specifically, to the source profile database. For example, this may occur the first time a user attempts to access the gateway device **12**. According to another aspect of the invention, where the source cannot be identified, the source may be directed to a login page in order to gather additional information to identify the source. For instance, the information may be entered with the aid of a webpage, a pop-up control panel or user interface, which can open when the source initially connects to the gateway device **12**, as effectuated by a home page redirection capability, described herein and in U.S. patent application Ser. No. 09/458,569, filed Dec. 8, 1999, entitled "Systems And Methods For Redirecting Users Having Transparent Computer Access To A Network Using A Gateway Device Having Redirection Capability" (referred to hereinafter as the "Redirection Application"), in U.S. patent application Ser. No. 09/458,579, filed Dec. 8, 1999, entitled "Systems And Methods For Redirecting Users Having Transparent Computer Access To A Network Using A Gateway Device Having Redirection Capability," and in U.S. patent application, Entitled "Systems and Methods for Redirecting Users Attempting to Access a Network Site," filed concurrently herewith, inventors Joel Short and Florence Pagan, the contents of each of which are incorporated herein by reference.

According to one aspect of the invention, the AAA server **30** can identify the source in communication with the gateway device in a manner that is transparent to computer users via a packet translation learned during a self configuration. That is, according to one aspect of the invention, a user will not be required to input identification, reconfigure the source computer or otherwise change the source computer's primary network settings. Furthermore, no additional configuration software will have to be added to the source computer. After a packet is received by the gateway device, attributes identified by the data packet can be compared with the data contained in the source profile database. Therefore, in addition to not requiring the reconfiguration of computers accessing the network, AAA servers of the present invention have the ability to authenticate sources without requiring interactive steps by the computer user, such as the entering of a user ID. For instance, the AAA server **30** may automatically identify the source based upon a MAC address, so that authorization of the source can be readily determined. Therefore, it will be appreciated that the AAA server **30** can determine the user, computer, or location from which the access is requested by comparing the attributes associated with the received data packet (such as in a header of the data packet) with data drawn from the source profile database. As will be described below, the access rights associated with the source may also be stored within the source profile database so that the system and method of the present invention can dynamically authorize access to particular services or destinations.

Once the source has established the network service connection via the authentication process discussed above, and a tunnel has been opened to facilitate a communication line between the source computer and a network, the gateway device **12** communicates with the AAA server **30** to assemble source profile information, or source-specific data. The source profile information that the gateway device assembles may include a MAC address, name or ID, circuit ID, billing scheme related data, service level data, user profile data, remote-site related data, and like data related to the source. As such, the AAA server **30** can transmit to the gateway device **12** any requisite information relating to the source's authorization rights and use of the network, as is next explained in detail.

In addition to authenticating users, the AAA server **30** of the present invention provides an authorization function, in which the source access rights are determined. The present invention enables dynamic authorization of sources, such that each source might have different respective network usage or access rights. After authentication, the AAA server **30** compares the attributes of the source with the access rights of the source associated with the user, computer, location or attribute(s). The access rights may be stored within the source profile database or within a separate subscription database located internal or external to the gateway device **12**. Therefore, separate databases may be utilized, where one stores identification information on sources for authentication, and another database stores the access rights of those sources that have been authenticated. However, because the profiles of all sources, identified by

attribute or a combination of attributes, are stored in a source profile database, it may be advantageous to locate information regarding access rights in the source profile database, which already contains information regarding each authenticated source, as described above.

According to one aspect of the invention the source profile database stores information defining the access rights of a source. For example, a source profile database may contain information indicating that a source having a particular MAC address has purchased pre-paid access, or that a given circuit ID has free access or unlimited access. Guests in a particular room or rooms of a hotel, for example, suites and penthouses, may receive free unlimited Internet access. Therefore, access rights can be available contingent upon the source's location (e.g. room) or location status (e.g. suite). In this event, no further identification is required, as the location from which the source is requesting access is known to the gateway device and stored in the source profile database.

In addition to storing information concerning what each source is authorized to access, the source profile database can also include specialized access information associated with a particular source, such as the bandwidth of the source's access, or a homepage to which the source should be directed. For example, a user accessing the network from a penthouse may receive a higher access baud rate than someone accessing the network from a typical hotel room. For example, where a user is transparently accessing the gateway device from a hotel room, the hotel network administrator may enter user access information into the source profile database based upon access rights associated with a room in the hotel. This can also be done automatically by the gateway device or a local management system, such as a hotel property management system, when the user checks into his or her room. Additionally, the user may establish the information to be contained within the source profile database upon first accessing the gateway device. For instance, a new user may be directed to enter a credit card number, e-wallet account information, pre-paid calling card number or like billing information to obtain access to the system. A source profile can also include historical data relating to a source's access to the network, including the amount of time a source has accessed the network. Specialized access or accounting information contained within the source profile database may be established by the system administrator, or by the source who has purchased or otherwise established access to the network.

According to one aspect of the invention, the authorization capability of the AAA server **30** can be based upon the type of services the source is attempting to access, such as a destination address, identified by the gateway device **12** based upon data received from the source computer. The destination can be a destination port, Internet address, TCP port, network, or the like. Moreover, the authorization capability of the AAA server **30** can be based upon the content type or protocol being transmitted. According to the system and method of the present invention, each packet can be filtered through the selective AAA process, so that any or all sources can be authorized access to a particular destination based on the access rights associated with the respective sources. Therefore, according to the present invention, each time the source attempts to access a different destination, the source is subject to the AAA, so the source may be prevented access from a particular site the AAA server **30** deems inaccessible to the source based upon the source's authorization. Alternatively, the AAA method according to the present invention allows some or all sources to connect directly to a specific site, such as credit card or billing servers for collecting billing information, which can collect payment or billing information so that the source profile can be updated and the source thereafter authorized access to networks. According to the system and method of the present invention, a source's authorization can also depend upon objective criteria, such as a specific time, so that the session can be terminated at a specific time, after a specific time has elapsed, or according to other dynamic information determined by the network provider. Furthermore, authorization can be associated with a combination of attributes. For example, a user may be authorized access to a network where the user has input the user's identification and has accessed the network from a particular room. Such a requirement could prevent unauthorized users also staying in a particular room from obtaining network access. Therefore, AAA can be based upon the origination, destination, and type of traffic.

By way of further explanation, a flow chart of the operation of the AAA server **30** will be described with respect to FIG. **2**, according to one aspect of the invention. In operation, a source computer requests (block **200**) access to a network, destination, service, or the like. Upon receiving a packet transmitted to the AAA server **30**, the AAA server **30** examines the packet to determine the identity of the source (block **210**). The attributes transmitted via the packet are temporarily stored in the source profile database so that the data can be examined for use in determining authorization rights of the source. The attributes contained in the packet can include network information, source IP address, source port, link layer information, source MAC address, VLAN tag, circuit ID, destination IP address, destination port, protocol type, packet type, and the like. After this information is identified and stored, access requested from a source is matched against the authorization of that source (block **230**).

Once a source profile has been determined by accessing the authorization rights stored in the source profile database, three possible actions can result. Specifically, once a source's authorization rights have been retrieved the AAA server **30** may determine a source to have access **222**, to be pending or in progress **224**, or to not have access **226**. First, a source is deemed valid (i.e., to have access) where the source profile database so states. If a source is determined to be valid, the source's traffic can be allowed to proceed out of the gateway device to the networks or online services the user associated with the source wishes to access (block **230**). Alternatively, the source may be redirected to a portal page, as described in the Redirecting Application, prior to being allowed access to the requested network. For example, a user may be automatically forwarded to a user-input destination address, such as an Internet address, for example, where a user has free access associated with the user's hotel room. Alternatively, this may occur where the user has already purchased access and the user has not exhausted available access time. Furthermore, an accounting message may be initiated **230** to log the amount of time the user is utilizing the gateway device such that the user or location may be billed for access.

If the second scenario occurs, in which the source is deemed pending **224** or in progress, the source may take steps to become authenticated (block **240**) so that the source information is recorded in the source profile database. For example, a user may have to enter into a purchase agreement, requiring the user to enter a credit card number. If the user needs to purchase access, or if the system needs additional information about the user, the user can be

redirected from the portal page via Home Page Redirect (HPR) and Stack Address Translation (SAT) to a location, such as a login page, established to validate new users. SAT and HPR can intervene to direct the user to a webserver (external or internal) where the user has to login and identify themselves. This process is described in detail in the Redirecting Application. After inputting any necessary and sufficient information, the user is then be permitted access to a destination address (block **230**, **250**). Where the information provided is insufficient the user will not be authorized access (block **260**). Finally, a third scenario can occur in which a source is deemed not to have access **226** so that the user is not permitted to access a destination via the network (block **260**).

Referring now to the accounting function of systems and methods of the present invention, upon authorizing a source network access, the AAA server **30** can register an accounting start to identify that the source is accessing the network. Similarly, when the source logs off or terminated the network session, an accounting stop can be registered by the AAA server **30**. Accounting starts or stops can be identified by the gateway device **12** or by the AAA server **30** upon a source's authentication or authorization to access a desired destination. Furthermore, accounting starts or stops can be registered in the source profile, or can be stored in a database separate from the AAA server **30** and located external to the network. Typically, accounting starts and stops include time stamps that indicate the amount of time a source has been accessing the network. Using this data, the time between the accounting start and accounting stop can be tallied so that the source's total connection time may be computed. Such information is valuable where the source is charged by an increment of time, such as an hour. A billing package, as are well known in the art, could then tally a user's total time accessing the network over a set period, such as each month, so that a bill can be created for the source. Because networks and ISPs often may charge a set rate for a specific duration of time (i.e., flat rate pricing), such as a month, regardless how much time is being spent accessing the network, accounting stops and starts may not be required for billing purposes. Nevertheless, accounting starts and stops may generally be recorded by the network provider or ISP for usage statistics.

An ISP or similar access provider would additionally benefit from being able to track subscriber's use of the ISP to establish bills, historical reports, and other relevant information. Preferably, the AAA server **30** is in communication with one or more processors for determining any fees which may be charged to the source, or due from the source, for network access or services. The AAA server **30** retrieves the historical accounting data in a real time basis or after a specific interval of time has elapsed. Preferably, the AAA server **30** retains such data in an easily accessible and manipulatable format such that the access provider (e.g., ISP) can produce reports representative of any desired type of historical data. For example, to project future use of the access provider, the AAA server **30** produces reports tallying the number of users accessing the Internet at certain time periods and from specific locales. Moreover, where the access provider provides alternative access to users, such as charging for faster connections (i.e., higher baud rate) for additional fees, the access provider may wish to analyze historical data using the AAA server **30** to best meet future customer demands. Such data may relate to network sessions currently on-going, the duration of those sessions, the bandwidth currently being used, the number of bytes that have been transferred and any other pertinent information. The AAA server **30** may be implemented using well known programs, such as Eclipse Internet Billing System, Kenan Broadband Internet Billing Software (manufactured by Lucent Technologies), or TRU RADIUS Accountant.

It will be appreciated that the AAA server **30** can dynamically account source access to a network in the same manner in which access is customizable on a source by source basis. That is, the AAA server **30** can maintain accounting records that vary depending upon the identity of a source, source location, source requested destination, or the like. Like the access or authorization rights, this information can be maintained in the source profile database or a similar accounting database. For instance, the AAA server **30** may determine that a particular source is only charged for accessing particular sites, and will only register an accounting site when those particular sites are accessed. Therefore, the AAA server **30** will identify account information stored in the subscriber's source profile to determine accounting starts, accounting stops, billing rates, and the like.

Many modifications and other embodiments of the invention will come to mind to one skilled in the art to which this invention pertains having the benefit of the teachings presented in the foregoing descriptions and the associated drawings. Therefore, it is to be understood that the invention is not to be limited to the specific embodiments disclosed and that modifications and other embodiments are intended to be included within the scope of the appended claims. Although specific terms are employed herein, they are used in a generic and descriptive sense only and not for purposes of limitation.

The invention claimed is:

1. A method for selectably controlling and customizing source access to a network, wherein the source is associated with a source computer, comprising:

receiving at the gateway device a request from the source computer for access to the network wherein the gateway device enables the source computer to access any network regardless of network configurations via a packet translation learned during a self configuration and no configuration software need be installed on the source computer to access the network;

identifying an attribute associated with the source based upon a packet transmitted from the source computer and received by the gateway device;

accessing a source profile corresponding to the source and stored in a source profile database, wherein the source profile is accessed based upon the attribute, and wherein the source profile database is located external to the gateway device and in communication with the gateway device, and

determining the access rights of the source based upon the source profile, wherein access rights define the rights of the source to access the network.

2. The method of claim **1**, wherein determining the access rights of the source based upon the source profile comprises determining the access rights of the source based upon the source profile, wherein access rights define the rights of the source to access a requested network destination.

3. The method of claim **1**, further comprising assigning a location identifier to the location from which requests for access to the network are transmitted, and wherein the location identifier is the attribute associated with the source.

4. The method of claim **1**, wherein accessing a source profile corresponding to the source comprises accessing a source profile stored in a source profile database, wherein the source profile database comprises a remote authentication dial-in user service (RADIUS).

5. The method of claim 1, wherein accessing a source profile corresponding to the source comprises accessing a source profile stored in a source profile database, wherein the source profile database comprises a lightweight directory access protocol (LDAP) database.

6. The method of claim 1, further comprising updating the source profile database when a new source accesses the network.

7. The method of claim 1, further comprising maintaining in the source profile database a historical log of the source's access to the network.

8. The method of claim 1, wherein the attribute associated with the source is based upon one of a MAC address, User ID or VLAN ID associated with the source computer from which the request for access to the network was transmitted.

9. The method of claim 1, wherein receiving at the gateway device a request from a source for access comprises the step of receiving a destination address from the source.

10. A system for selectably controlling and customizing access, to a network, by a source, where the source is associated with a source computer, and wherein no configuration software need be installed on the source computer to access the network, comprising:

a gateway device, wherein the gateway device receives a request from the source for access to the network and provides the source computer with access to the network regardless of network configurations via a packet translation learned during a self configuration;

a source profile database in communication with the gateway device and located external to the gateway device, wherein the source profile database stores access information identifiable by an attribute associated with the source, and wherein the attribute is identified based upon a data packet transmitted from the source computer and received by the gateway device, and

an Authentication, Authorization and Accounting (AAA) server in communication with the gateway device and source profile database, wherein the AAA server determines if the source is entitled to access the network based upon the access information stored within the source profile database, and wherein the AAA server determines the access rights of the source, wherein access rights define the rights of the source to access destination sites via the network.

11. The system of claim 10, wherein the packet received by the gateway device include at least one of VLAN ID, a circuit ID, and a MAC address.

12. The system of claim 10, wherein the source profile database comprises a remote authentication dial-in user service (RADIUS).

13. The system of claim 10, wherein the source profile database comprises a lightweight directory access protocol (LDAP) database.

14. The system of claim 10, wherein the source profile database includes a plurality of source profiles, wherein each respective source profile of the plurality of source profiles contains access information.

15. The system of claim 14, wherein each respective source profile contains historical data relating to the duration of network access for use in determining the charges due for the network access.

16. The system of claim 10, wherein the source profile database is located within the AAA server.

17. A method for redirecting a source attempting to access a destination through a gateway device, wherein source is associated with a source computer, and wherein the gateway device enables the source to communicate with a network, comprising:

receiving at the gateway device a request from the source to access the network regardless of network configurations via a packet translation learned during a self configuration and without requiring the source computer to include network software configured for the network;

identifying the source based upon an attribute associated with the source;

accessing a source profile database located external to the gateway device, the source profile database storing access rights of the source;

determining the access rights of the source based upon the identification of the source, wherein the access rights define the rights of the source to access destination sites via the network; and

directing the source to a redirection site when the source profile is not located within the source profile database.

18. The method of claim 17, wherein accessing a source profile database comprises accessing a source profile database comprising a remote authentication dial-in user service (RADIUS).

19. The method of claim 17, wherein accessing a source profile database comprises accessing a source profile database comprising a lightweight directory access protocol (LDAP) database.

20. The method of claim 17, further comprising assigning a location identifier to the location from which requests for access to the network are transmitted, and wherein the location identifier is the attribute associated with the source.

21. The method of claim 17, further comprising updating the source profile database when a new source accesses the network.

22. The method of claim 17, further comprising maintaining in an accounting database a historical log of the source's access to the network, wherein the accounting database is in communication with the source profile database.

23. The method of claim 17, wherein receiving at the gateway device a request from a source for access comprises the step of receiving a destination address from the source.

24. The method of claim 19, wherein determining if the source computer is entitled to access the destination address further comprises denying the source computer access where the source profile indicates that the source computer is denied access.

* * * * *

US006868399B1

(12) **United States Patent**
Short et al.

(10) **Patent No.: US 6,868,399 B1**
(45) **Date of Patent: Mar. 15, 2005**

(54) **SYSTEMS AND METHODS FOR INTEGRATING A NETWORK GATEWAY DEVICE WITH MANAGEMENT SYSTEMS**

(75) Inventors: **Joel E. Short**, Los Angeles, CA (US); **Denis I. Perelyubskiy**, Van Nuys, CA (US)

(73) Assignee: **Nomadix, Inc.**, Westlake Village, CA (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 427 days.

(21) Appl. No.: **09/693,061**

(22) Filed: **Oct. 20, 2000**

Related U.S. Application Data

(60) Provisional application No. 60/160,973, filed on Oct. 22, 1999, provisional application No. 60/161,182, filed on Oct. 22, 1999, provisional application No. 60/161,139, filed on Oct. 22, 1999, provisional application No. 60/161,189, filed on Oct. 22, 1999, provisional application No. 60/161,181, filed on Oct. 22, 1999, and provisional application No. 60/161,093, filed on Oct. 22, 1999.

(51) **Int. Cl.**[7] **G06F 17/60**
(52) **U.S. Cl.** **705/34**; 709/224
(58) **Field of Search** 705/34; 709/224

(56) **References Cited**

U.S. PATENT DOCUMENTS

5,612,730	A		3/1997	Lewis	
5,745,884	A	*	4/1998	Carnegie et al.	705/34
5,802,502	A	*	9/1998	Gell et al.	705/34
5,852,812	A	*	12/1998	Reeder	705/34

(List continued on next page.)

FOREIGN PATENT DOCUMENTS

EP	0 762 707 A2		3/1997	
JP	2000-354127 A	*	12/2000	H04N/1/00
JP	2002-111870 A	*	4/2002	H04M/3/42
WO	WO 98/16044		4/1998	

OTHER PUBLICATIONS

"Atreus Systems Corporations and B2B Connect, Inc. Partner to Deliver Bundled Broadband Services to Multi– Tenant, High Ri Buildings", Feb. 14, 2000, Business Wire.*

"NetGame Ltd. Announces its High–Speed, In–Room Hotel Internet Access Product to be Displayed at HITEC 99", Jun. 16, 1999, Business Wire.*

"Copper Mountain Introduces CopperPowered Hotel Initiative to Deliver Cost–effective Always–on or Usage–based Broadband Access to Hotel Guests", Dec. 6, 1999, Business Wire.*

"Nomadix Joins Copper Mountain Networks to Provide High–Speed Internet Access to Hotels Guests", Dec. 6, 1999, Business Wire.*

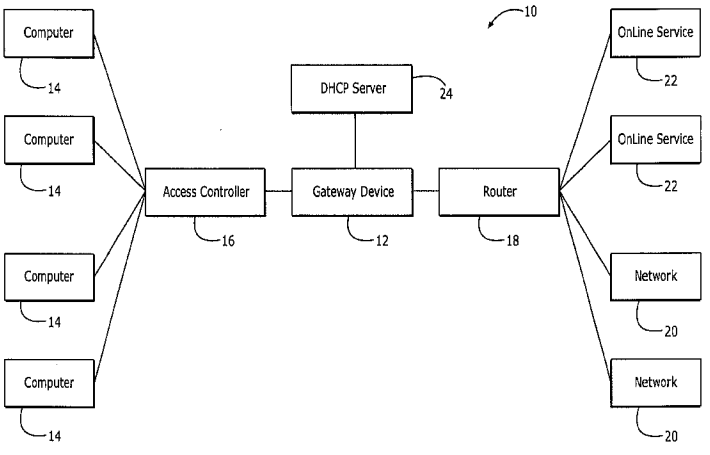
(List continued on next page.)

Primary Examiner—Bryan J Jaketic
(74) *Attorney, Agent, or Firm*—Alston & Bird LLP

(57) **ABSTRACT**

Systems and methods enabling a management system to communicate with a network gateway device to automatically manage a user accessing a computer network, such as a local network. The system includes a computer, and a network gateway device in communication with the computer for connecting the computer to a computer network, wherein the network gateway device maintains data representative of the user's access to the computer network and wherein the network gateway device reconfigures the data. The system also includes a management system connected to said network gateway device for automatically billing the user based upon usage of the computer network, wherein the management system is configured to communicate according to at least one compatible protocol. The network gateway device reconfigures the data to meet one of the predetermined protocols supported by the management system, and the management system receives the data reconfigured by the network gateway device and utilizes the data reconfigured by the network gateway device for automatic billing purposes.

21 Claims, 3 Drawing Sheets



U.S. PATENT DOCUMENTS

5,864,610	A		1/1999	Ronen	
5,893,077	A	*	4/1999	Griffin	705/34
5,950,195	A		9/1999	Stockwell et al.	
5,987,430	A	*	11/1999	Van Horne et al.	705/34
6,119,160	A	*	9/2000	Zhang et al.	709/224
6,208,977	B1	*	3/2001	Hernandez et al.	705/34
6,338,046	B1	*	1/2002	Saari et al.	705/34
6,349,289	B1	*	2/2002	Peterson et al.	705/34
6,496,850	B1	*	12/2002	Bowman-Amuah	709/224

OTHER PUBLICATIONS

"Ascend Communications and ATCOM/INFO Announce Development Alliance", Jun. 22, 1999, Business Wire.*

Schoen et al., *Convergence Between Public Switching and the Internet*, published Sep. 21, 1997 in *XVI World Telecom Congress Proceedings*, pp. 549–560.

* cited by examiner

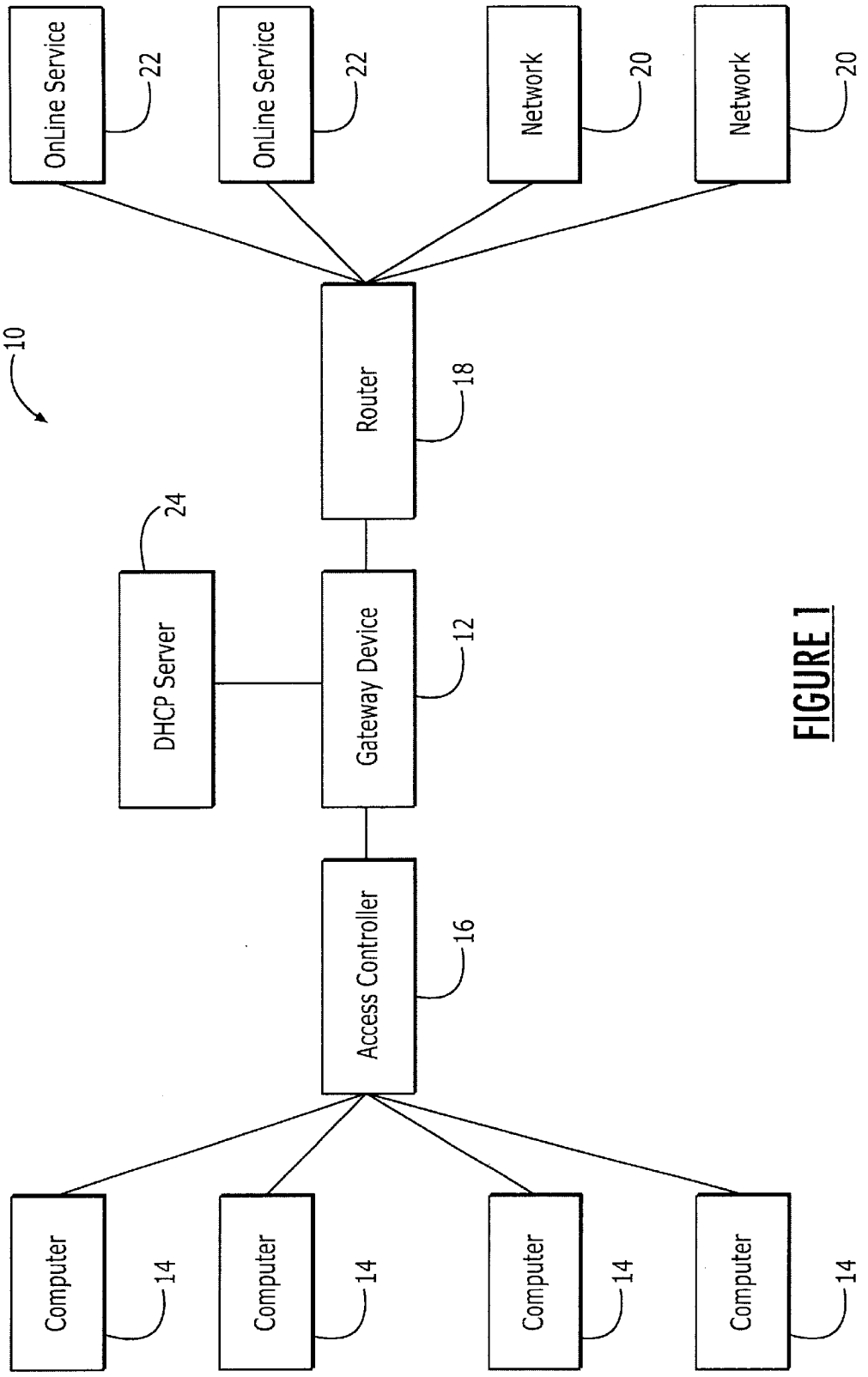

OnLine Service
22
OnLine Service
22
Network
20
Network
20
10
Router
18
DHCP Server
24
Gateway Device
12
Access Controller
16
Computer
14
Computer
14
Computer
14
Computer
14

FIGURE 1

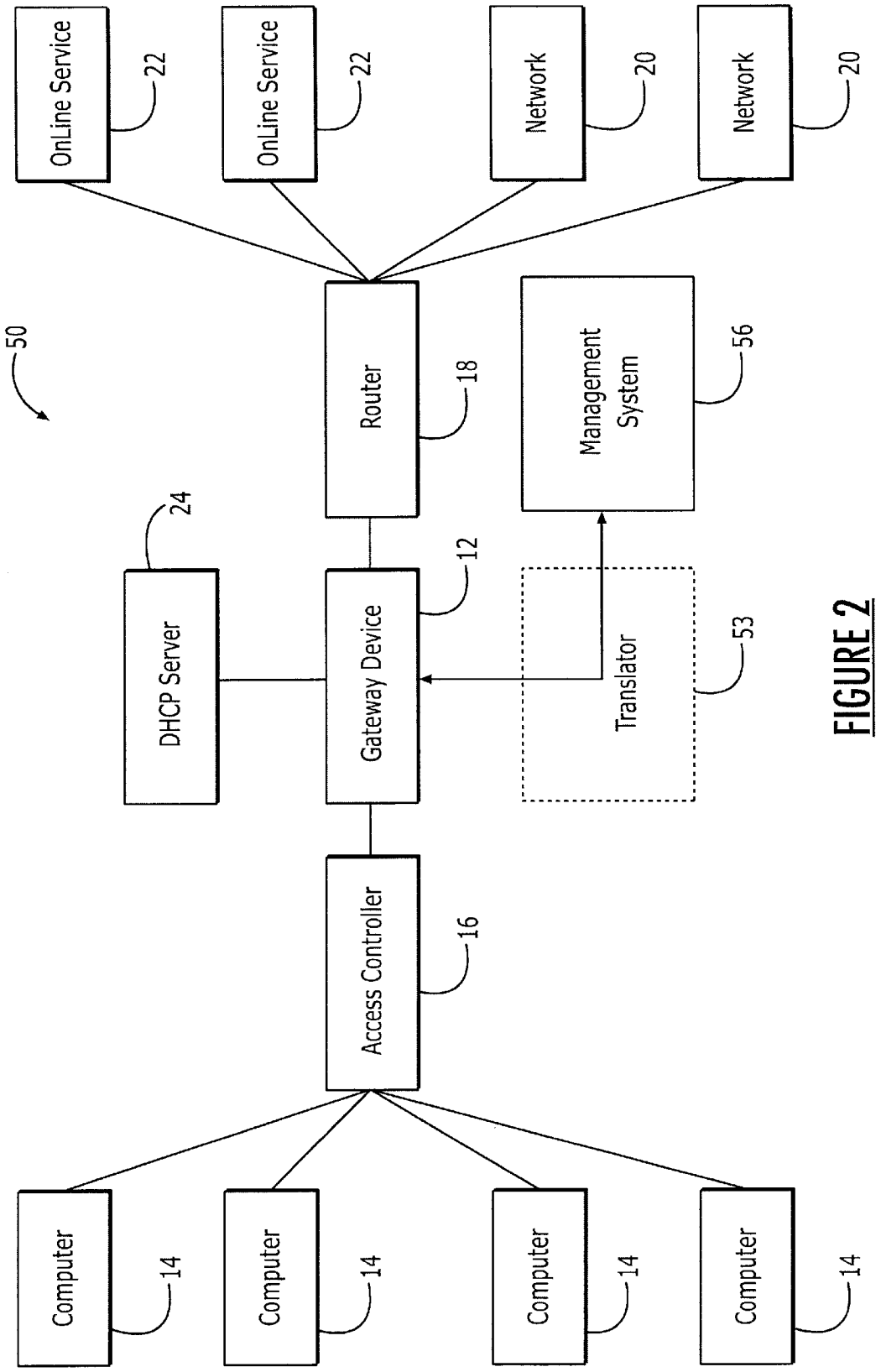

OnLine Service
22
OnLine Service
22
Network
20
Network
20
50
Router
18
Management System
56
24
DHCP Server
12
Gateway Device
Translator
53
Access Controller
16
Computer
14
Computer
14
Computer
14
Computer
14

FIGURE 2

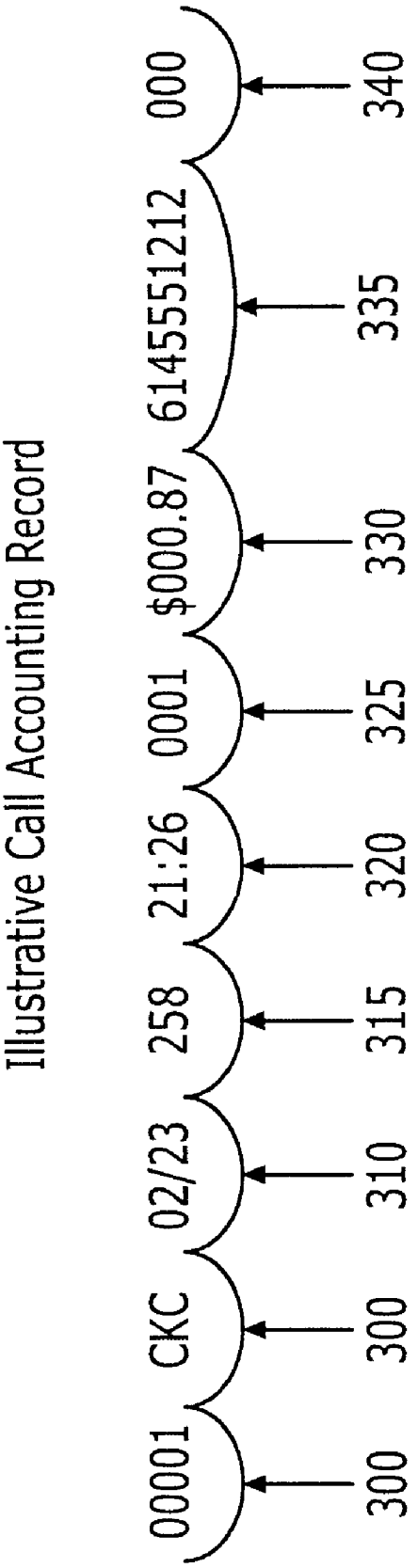

Illustrative Call Accounting Record
00001
300
CKC
300
02/23
310
258
315
21:26
320
0001
325
$000.87
330
6145551212
335
000
340

FIGURE 3

SYSTEMS AND METHODS FOR INTEGRATING A NETWORK GATEWAY DEVICE WITH MANAGEMENT SYSTEMS

CROSS-REFERENCE TO RELATED APPLICATIONS

The present invention claims priority from U.S. Provisional Application Ser. No. 60/160,973, filed Oct. 22, 1999, titled "Systems and Methods for Enabling Network Gateway Devices to Communicate with Management Systems to Facilitate Subscriber Management," U.S. Provisional Application Ser. No. 60/161,182, filed Oct. 22, 1999, entitled "Systems and Methods for Dynamic Bandwidth Management on a Per Subscriber Basis in a Computer Network," U.S. Provisional Application Ser. No. 60/161,139, filed Oct. 22, 1999, titled "Information And Control Console For Use With A Network Gateway Interface," U.S. Provisional Application Ser. No. 60/161,189, filed Oct. 22, 1999, titled "Systems and Methods for Transparent Computer Access and Communication with a Service Provider Network Using a Network Gateway Device," U.S. Provisional Application Ser. No. 60/161,181, filed Oct. 22, 1999, titled "Gateway Device Having an XML Interface and Associated Method," and U.S. Provisional Application Ser. No. 60/161,093, filed Oct. 22, 1999, titled "Location-Based Identification and Authorization for use With a Gateway Device," the contents of each of which are incorporated herein by reference.

FIELD OF THE INVENTION

The present invention relates generally to a network gateway device and, more particularly, to systems and methods for integrating one or more gateway devices with management systems.

BACKGROUND OF THE INVENTION

Through gateway devices or routers Internet Service Providers (ISPs) or enterprise network (such as a LANS) providers can permit a wide variety of users access to their networks and to other online services. Because high speed access to enterprise networks, the Internet and on-line services is a desirable commodity, like long distance telephone service, costs associated with the service are typically passed on to the remote user/subscriber. Therefore, in many instances the remote user/subscriber is concerned with being able to acquire network access and service in the most cost efficient and convenient manner.

In this regard, service concerns of subscribers accessing local networks through gateway devices parallel those concerns of customers utilizing internet service providers for conventional telephone line dial-up Internet access. In both cases, users typically want inexpensive, flexible and customer friendly service options. Correspondingly, a gateway device administrator desires the capability to be able to offer the user/subscriber numerous and different service and billing rate options, like those available in conventional dial-up internet access. For example, the remote user in a hotel environment may desire a subscription for only a day, or for the duration of their stay at the hotel. The user/subscriber may be charged on an hourly rate, a daily rate, a weekly rate, or at any other interval. Such flexible plans offer cost savings to consumers and are an attractive incentive to lure customers into buying access time to the enterprise network, online services or the internet.

Unlike conventional dial-up internet access, however, gateway devices permit remote users to access various

computer networks and on-line services without having a prior service contract or an ongoing relationship with the service provider. Therefore, unlike conventional dial up access plans, which can bill subscribers on a set monthly schedule, gateway devices make recouping remote access charges more challenging. This is especially true for nomadic users, who may utilize a remote connection to a network only once before relocating. Once the traveler has moved onward, the network provider may have difficulty in collecting any unpaid service charges. Furthermore, billing of nomadic users is another hurdle to fast and easy access to the enterprise network, on-line services and the internet. The benefits of remote plug and play access therefore may be overshadowed by time consuming payment methods. For example, where a user is required to complete an onerous billing procedure to pre-purchase local network time or to pay for the network use after each session, the user may decide not to use the network. Thus, any convenience provided by the computer network is superceded by the inconvenient billing method.

Gateway device administrators also desire convenient methods in which to bill users/subscribers. Because the gateway device enables subscribers immediate plug and play connections to computer networks, such as hotel or airport networks, the computer network provider and/or service provider of the high speed network would like to quickly and immediately bill the users/subscribers. This billing should be able to easily track a user/subscriber's usage of the network so as to recoup costs for the network hardware and network connection. Furthermore, such billing should be automated such that system administrators do not need to individually bill each user.

Therefore, it is desirable for customers, network providers and service providers to implement automatic billing through a gateway device utilizing a management system already used for billing customers. Such automatic billing utilizing the present invention to automatically send a billing record to a management system would benefit customers by facilitating fast and easy access, and also would benefit network providers who could appropriately charge customers for obtaining network or Internet access.

SUMMARY OF THE INVENTION

The present invention relates generally to a network gateway device and, more particularly, to network gateway devices communicating with management systems or servers, such as hotel property management systems, to facilitate subscriber management and billing.

According to one embodiment of the invention, there is provided a system for enabling a management system to communicate with a network gateway device in order to automatically bill a user for access to a computer network such as a local network or the Internet. The system includes a computer, and a network gateway device in communication with the computer for connecting the computer to a computer network and for maintaining data representative of the user's access to the computer network. The system also includes a management system connected to the network gateway device that is designed to automatically bill the user for network or Internet access, or services facilitated by the network access, such as room service, business services, and the like. The management system is also designed to communicate with a third party device according to at least one predetermined protocol. According to the present invention, the gateway device is therefore designed to supply billing data using one of the predetermined protocols supported by

the management system. As such, the management system receives the billing data supplied by the network gateway device and utilizes the data for automatic billing purposes.

Furthermore, in the system for enabling a management system to communicate with a network gateway device to bill a user for access to a computer network, the management system can be located within the computer network. Additionally, the system can include a translator in communication with the gateway device and management system for receiving the data supplied by the network gateway device. The translator can further reconfigure the supplied billing data received from the network gateway device, and can transmit the further reconfigured data to the management system. The data representative of the user's access to the computer network can include data representative of the user's location, access time, date which access was obtained, billing rate, and other pertinent information.

According to another embodiment of the invention, a method for enabling a remote server, such as an Internet website, to communicate with a network gateway device in order to automatically bill a customer via the management system such as a hotel's Property Management System.

According to yet another embodiment of the present invention, there is disclosed a system for integrating a gateway device with a management system, wherein the management system can activate communication with the gateway device. The system includes a computer, and a network gateway device in communication with said computer for connecting the computer to the computer network, wherein the network gateway device maintains data representative of the user's access to the computer network. The system further includes a management system connected to said network gateway device, wherein the management system receives the data representative of the user's access to the computer network, and wherein the management system initiates communication with the gateway device to manage the computer network.

According to one aspect of the invention, the management system communicates with the network gateway device in at least one predetermined protocol selected from the group consisting of a low level protocol, a call accounting record, and a private branch telephone system protocol. According to another aspect of the invention, the management system is a hotel property management system.

The ability to bill customers for service automatically and track customers without administrator intervention allows the local network service provisioning to be done economically, efficiently, and securely, as no administrator intervention is required. That is, the gateway device generates accounting records that are formatted and forwarded to the PMS to facilitate automatic billing. This automatic billing generates a bill that can be paid by a customer electronically (e.g., via the Internet), or at checkout of the hotel. Alternatively, a customer may have pre-purchased network access.

The present invention provides an: incentive for hotels, airports, and other computer networks to provide network connections to users because the computer network has a captive customer base. Furthermore, automatic billing can enable usage-based billing for network access and services, which is desirable to customers. Finally, automatic billing can reduce the risk of network use by an unauthorized user.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. **1** is a block diagram of a computer system including a gateway device facilitating communication between computers and networks or other online services, according to one embodiment of the invention.

FIG. **2** shows a block diagram of the computer system of FIG. **1**, including a gateway device integrated with a management system, according to one aspect of the invention.

FIG. **3** shows a call accounting record generated by the gateway device, according to one embodiment of the present invention.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

The present invention now will be described more fully hereinafter with reference to the accompanying drawings, in which preferred embodiments of the invention are shown. This invention may, however, be embodied in many different forms and should not be construed as limited to the embodiments set forth herein; rather, these embodiments are provided so that this disclosure will be thorough and complete, and will fully convey the scope of the invention to those skilled in the art. Like numbers refer to like elements throughout.

Referring now to FIG. **1**, there is shown in block diagram form a computer system **10** including a plurality of computers **14** that can communicate with one or more online services **22** or networks via a gateway device **12** providing the interface between the computers **14** and the various networks **20** or online services **22**. One embodiment of such a gateway device has been described in U.S. patent application Ser. No. 08/816,174 and U.S. Provisional Application No. 60/111,497 (collectively referred to herein as the Gateway Device Applications), the contents of which are incorporated herein by reference. Briefly, the gateway device **12** facilitates transparent computer access to the online services **22** or networks **20**, such that the computers **14** can access any networks via the device **12** regardless of their network configurations. Additionally, the gateway device **12** includes the ability to recognize computers attempting to access a network **20**, the location of computers attempting to access a network, the identity of users attempting to gain network access, and additional attributes, as is discussed in the Gateway Device Applications.

As illustrated in FIG. **1**, the computer system **10** also includes an access concentrator **16** positioned between the computers **14** and the gateway device **12** for multiplexing the signals received from the plurality of computers onto a link to the gateway device **12**. Depending upon the medium by which the computers **14** are connected to the access concentrator, the access concentrator **16** can be configured in different manners. For example, the access concentrator can be a digital subscriber line access multiplexer (DSLAM) for signals transmitted via regular telephone lines, a cable head end (a Cable Modem Termination Shelf (CMTS)) for signals transmitted via coaxial cables, a wireless access point (WAP) for signals transmitted via a wireless network, an Ethernet switch or the like.

The computer system **10** further includes one or more routers **18** and/or servers (not shown in FIG. **1**) to control or direct traffic to and from a plurality of computer networks **20** or other online services **22**. While the computer system **10** is depicted to have a single router, the computer system **10** can have a plurality of routers, switches, bridges, or the like that are arranged in some hierarchical fashion in order to appropriately route traffic to and from the various networks **20** or online services **22**. In this regard, the gateway device **12** typically establishes a link with one or more routers. The routers, in turn, establish links with the servers of the

networks **20** or online services **22**, based upon the user's selection. It will be appreciated by one of ordinary skill in the art that one or more devices illustrated in FIG. **1** may be combinable. For example, although not shown, the router **18** may be located entirely within the gateway device **12**. Furthermore, additional elements may be included in the computer system **10**, such as elements disclosed in the Gateway Device Application, or network elements known to those of ordinary skill in the art.

FIG. **2** shows a block diagram of the computer system **50** of FIG. **1**, integrated with a management system **56**, according to one embodiment of the present invention. It will be appreciated by those of skill in the art that the embodiment shown in FIG. **2** is for illustrative purposes, and that the gateway device **12** may be integrated with virtually any network server or management system, such as computer networks used in corporate offices, airports, arenas, apartment complexes, office buildings or the like. As a result, the embodiment shown in FIG. **2** is for illustrative purposes only, and is not intended to limit the scope of the present invention.

According to one aspect of the invention, the gateway device **12** is in direct communication with the management system **56** through a serial connection **57**. Optionally, the gateway device **12** may be connected to the management system **56** through a translator **53**, illustrated with phantom lines to indicate that the translator **53** is not a required component of the management system **56**, as is explained in detail below. Because the gateway device **12** comprises similar components to the system illustrated in FIG. **1**, it will be appreciated that the systems can be implemented in like manners with like components. Furthermore, additional embodiments of the present invention discussed with respect to FIG. **1** and in the Gateway Device Applications may also be implemented in the system **56** shown in FIG. **2**.

As shown in FIG. **2**, each of the plurality of computers **14** is located in a different hotel room **60**, **70**, **80** and **90** to allow multiple guests to access the hotel's computer network. The computers **14** are connected to the access controller **16** through a communications port in each room using a communications device such as a DSL modem, an Ethernet card, a coaxial cable, or another well known communication device. Most preferably, the connection between the computers **14** and the access controller **16** is a high speed connection, so that the computers **14** can receive data as fast as the gateway device **12** can forward the data. The data transmitted from the gateway device **12** to the computers **14** may originate from any devices located within the computer system **50**, such as communications via the Internet.

Management systems **56** are typically implemented through the use of one or more conventional computers. It will be appreciated that management systems **56** may include any well known computer based systems implemented in hotels, airports, arenas or other venues to manage operations or network access. For instance, where the gateway device **12** is located in a corporate office the gateway device **12** may be in communication with one or more central servers to which all computers in the corporate office are connected. In the embodiment of FIG. **2**, the management system **56** can be a property management system located within a hotel. Typical hotel property management systems automate operations such as room reservations, room assignments, guest check-in and check-out, and other front desk activities. Furthermore, typical hotel property management systems maintain a log of telephone calls and telephone charges for each guest room, and are in communication with the Internet to facilitate on-line reservation systems.

Where the management system **56** is illustrative of a property management system in a hotel, the gateway device **12** is in communication with the management system **56** such that each user/subscriber's access and connection to the hotel network via the gateway device **12** can be monitored by the management system **56**. Typically, the gateway device **12** is connected via a serial connection **57**, Ethernet connection, or LAN to the management system **56**. According to one preferred embodiment the gateway device **12** is connected to the management system **56** via a serial interface. The connection may operate at a variety of baud rates, such as at 9,600 or 56,000 bits per second, or at much higher rates. The primary purpose for integrating the gateway device **12** with the management system **56** is to allow the hotel to bill each specific user/subscriber for their use and connection to the hotel's network or to automatically bill such use directly to the room from which access was obtained. As disclosed in detail in the Gateway Device Applications, the identity of a user or a location from which a user communicates with the network can be determined by the gateway device **12**. According to one aspect of the invention, a user will not be authorized access to networks **20** or online serves **22** until the user is authorized access. This may require a user to enter a user name and ID to identify the user, or may require registration (e.g., input of a credit card number) or pre-payment for use of the system. Furthermore, the user may be authenticated based upon the AAA process described in U.S. patent Application titled "Systems And Methods For Providing Dynamic Network Authorization, Authentication And Accounting," inventors Joel Short and Florence Pagan, the contents of which are incorporated herein by reference. As described in the application, the gateway device **12** can identify users based upon the user's computer, location, or computer from which access is requested.

The gateway device **12** can thus monitor and record information such as the identity of the user, the room from which the user obtained access, the amount of time that the user utilized the network, the cost of each network access, the time, date and duration of the network access, and other additional information. Through this integration, systems of the present invention offer user/subscribers of computer networks integrated with management systems convenient payment plans in which users do not have to pre-pay for network access or physically pay each time the network is accessed, and features, such as billing status, that are otherwise available only by directly accessing management systems.

Traditional hotel property management systems are configured to communicate with various third party systems, such as point of sale systems, PBX systems, pay per view systems, and credit card authorization servers through serial ports, modem communications, dedicated connections, or through other well known communication means. Such connections allow the management system **56** to function as a fully integrated system, which allows customers to use a variety of hotel resources while automatically being billed for each transaction. Hotel property management systems are generally configured to receive such communications because these third party systems are typically used in the vast majority of hotels. To receive data from each of these third party systems, management systems typically include software for communicating with the third party systems based upon the data protocol and data structure implemented by the management system. The software allows data from third party systems to be received and reconfigured, if necessary, so that the data is in a format appropriate to be

utilized by the management system. However, because typical management systems that are currently deployed are not designed to receive data from a gateway device **12**, the gateway device **12** can be designed to interface with the management system **56** without requiring additional programming of the management system software.

For instance, it will be appreciated by those of skill in the art that the information passed from the gateway device **12** to the management system **56** can be configured, in most respects, identical to information received by the management system **56** from a private branch telephone system (PBX), which are commonly utilized in hotels. PBX systems allow room to room, local and long distance telephone calls to be made by guests, and are typically connected to hotel property management systems to facilitate billing of hotel guests based upon the room in which the call is made. Charges for calls can then be paid by the guest upon checkout, automatically billed to the guest's credit card or automatically billed to the guest with room charges. Although the gateway device **12** may be configured to communicate with the management system **56** in the same manner as PBX systems, it will be appreciated that this configuration is not required by the present invention. However, such a configuration is preferred such that the gateway device can be integrated in existing hotels with minimum or no impact on the configuration of preexisting management system equipment. Because the gateway device **12** can communicate with management systems by any means well known to those of skill in the art for transmitting network access and usage data to management systems, it will be appreciated that the device **12** can be configured in any manner that results in the least significant impact on management systems or on the user or administrator.

Therefore, in a preferred embodiment the gateway device **12** of the present invention formats data such that the data has the same data protocol and data structure as that of a third party service, such as a PBX, that the management system **56** is designed to receive. The management system **56** is adapted to communicate using different protocols specific to different types of devices or third party systems. Thus, the gateway device **12** can masquerade as a PBX or another third party system. The gateway device **12** creates a data record corresponding to an individual user/subscriber's use of the computer system, including the user/subscriber's location (room number), access charge, and additional information, as discussed above. The gateway device **12** formats the data record to fit the proper format required by the property management system vendor. The data is then transmitted to the management system **56** using low level protocol format. Typically, such formats are well known to those of skill in the art of management system design. According to one embodiment of the invention, the gateway device **12** can format the data as a call accounting record (CAR), illustrated in FIG. **3**.

The CAR of FIG. **3** is in a standard PBX format that the gateway device **12** can modify as needed to conform to the format requested by the management system **56**. The CAR includes data representative of month/day **310**, extension/room **315**, time **320**, duration **325** (e.g., in minutes), charge **330**, phone number **335**, routing code **340**, and the like, as well as additional data **300** that may be necessary for accurate ordering, transmittal and/or reception of the call accounting record. It will be appreciated that additional formats containing similar data can also be generated by the gateway device **12** for transmission to the management system **56**. Because management systems can differ, each system utilizing different user interfaces, variables, and operating systems, the gateway device **12** should communicate data to the management system **56** using data formats acceptable to a large number of management systems. In this manner, the gateway device **12** may be compatible with a majority of property management systems. For example, the gateway device **12** may be compatible to operate with the most popular management systems and formats, such as Micros Fidelio (manufactured by MICROS Systems, Inc., Beltsville, Md.), HOBIC, Autoclerk (manufactured by AutoClerk, Inc., Lafayette, Calif.), and other well known systems and formats.

However, there are many different management system standards, none of which are universal and implemented in all property management systems. As a result, although the gateway device **12** can be configured to conform to a large number of differing management systems, the gateway device **12** is set up to communicate with the management system in which is integrated. Furthermore, it will be appreciated that although the gateway device **12** may include a number of configuration settings, the device may not be able to conform to some systems. As a result, a translator **53** may be optionally used to manipulate the data output by the gateway device **12** in such a manner as to allow the data to be utilized by the management system **56**. In one embodiment, the translator may comprise a Lodging Link II device (LL) (manufactured by Protocol Technologies, Inc., Scottsdale, Ariz.) to convert incoming data from the gateway device **12** to data acceptable to the property management system device, such as UHALL protocol. Additionally, the translator **53** may also be connected to one or more devices or systems in =communication with the property management system, such as the pay per view system or credit card authorization system, to format data output by any system or component having data protocols which differ from those of the management system **56**.

Additionally, according to one aspect of the invention, it should be appreciated that a gateway device **12** in located within a network may not have a relationship with a billing company, and as a result, the gateway device **12** may not obtain a CAR from a third party. In this instance, a management system **56** can rely on the gateway device **12** to create its own call accounting record that can be sent to a standard printer. The printed data (call accounting record generated by the gateway device **12**) can then be manually entered into the management system accounting records, such as a hotel/business accounting record, and thus added to the user's bill.

Because data may be transferred to the management system in a CAR format, data typically within such format must be altered to accurately reflect the computer network service being provided to the user/subscriber. For example, in PBX systems, CAR format usually includes the phone number to which a telephone call is being made. However, when a user/subscriber is obtaining access to the hotel network via the gateway device **12**, no telephone number is dialed or called. Therefore, when possible, data within the CAR format (i.e., telephone record), such as telephone numbers, may be replaced with a descriptive record that indicates some other data that the property management systems wishes to track or record. On the other hand, where the CAR records cannot be replaced, a mock field, such as a mock telephone number, may be included so that the property management system receives the entire record it is programmed to receive. Thereafter, the mock number is not utilized by the management system **56**. Additional problems may also exist, for example, where the management system

56 is not devised to support the normumeric ASCII characters typically transmitted by the gateway device **12**. In this situation, the gateway device can be configured to replace the ASCII characters with numeral designations.

Integrating the gateway device **12** with the management system **56** allows a user/subscriber's account to be billed directly to that user?s hotel bill in a like manner as telephone calls billed to a hotel room. For example, where the management system **56** receives data representing a user's access to the local system, from the gateway device **12** and as described in the Gateway Device Applications, the management system **56** can automatically bill the operator through the use of a credit card authorization system in communication with the management system **56**. It will be appreciated that this can be accomplished because the property management system can register network access, identified by the gateway device, in one or more fields existing or established in the management system **56**. For instance, the management system **56** can register network access as a long distance call, or can establish a special fee for such access and add the cost of that access to a customer's bill in the same manner as a long distance call. In this manner, the customer's payment can be fast, easy, automated and transparent to the user.

Additionally, once the data transmitted by the gateway device **12** is received by the management system **56**, the management system **56** can display the data using a management system **56** interface. Preferably, the data may be displayed in a easily readable and printable form to allow a user/subscriber to view a summary of access information. Moreover, the data should be accessible to the user/subscriber's accounting record. In this manner, charges due to network access may be automatically placed on a customer's pre-existing bill, such as a hotel bill. Where access is obtained at another location, such as at an airport, the airport system manager (i.e., equivalent to the hotel property management system in the above example) may automatically bill the customer, can automatically charge the customer's credit card, or can add the charges to an account which the customer maintains. In this regard, while the management system has primarily been described in conjunction with a hotel computer network, the management system can be utilized in a variety of other applications in which a user/subscriber obtains access to a computer network or other on-line service via a gateway device.

Although the invention has been described herein as using a gateway device to monitor and facilitate network access of a user, and to transmit accounting information to the management system, it will be appreciated that the gateway device **12** can also be used to account for a variety of charges incurred as a result of the user's interaction with online services **22** or networks **20**. For instance, a remote system can bill the user directly to the management system. This could occur, for instance, where the user orders goods or services online. In this event, the gateway device can add the charge directly to the user's account in the management system.

Additionally, although the management system has been discussed herein as receiving data from the gateway device, in a passive manner, the management system can additionally transmit information to the user or gateway device **12**. Therefore, the management system can activate communication with the gateway device **12** to aid in managing the computer network. For instance the management system may inform the gateway device **12** that a particular room or user should be allowed or denied access to the system **50**, or that a particular port should be turned on or off. Additionally, the management system may request information from the gateway device, such as whether or not a particular user is using the system. This request may be automated or facilitated by a network administrator. Therefore, it will be appreciated that the system **50** may operate both downstream (from the user/computer or network or online service to the management system) and upstream (from the management system to the user/computer or online service or network.)

Many modifications and other embodiments of the invention will come to mind to one skilled in the art to which this invention pertains having the benefit of the teachings presented in the foregoing descriptions and the associated drawings. Therefore, it is to be understood that the invention is not to be limited to the specific embodiments disclosed and that modifications and other embodiments are intended to be included within the scope of the appended claims. Although specific terms are employed herein, they are used in a generic and descriptive sense only and not for purposes of limitation.

That which is claimed:

1. A system for integrating a gateway device with a management system to automatically bill a user for access to a computer network, comprising:

a computer;

a network gateway device in communication with said computer for connecting the computer to the computer network, wherein the network gateway device communicates with the computer absent additional agents implemented by the computer and wherein the network gateway device maintains data representative of the user's access to the computer network; and

a management system connected to said network gateway device for automatically billing the user based upon usage of the computer network, wherein said management system is configured to communicate according to at least one predetermined protocol,

wherein the network gateway device formats the data into call accounting record format, and wherein said management system receives the data formatted by the network gateway device and utilizes the data formatted by the network gateway device for billing purposes.

2. The system of claim **1**, further comprising a translator in communication with the gateway device and management system for receiving the data reconfigured by the network gateway device, said translator adapted to further reconfigure the reconfigured data, and to transmit the further reconfigured data to the management system.

3. The system of claim **1**, wherein the data representative of the user's access to the computer network comprises data representative of the user's location.

4. The system of claim **1**, wherein said management system is a hotel property management system.

5. The system of claim **1**, wherein the management system stores data reconfigured by the network gateway device, and wherein at least some of said data is accessible by the computer.

6. A method for integrating a gateway device with a management system to automatically bill a customer for access to a computer network, comprising:

enabling a user to access, via a network gateway device, a computer network absent additional agents implemented by a user's computer;

collecting data corresponding to the user's access to said computer network in said network gateway device;

reconfiguring said data into call accounting record format; and

transmitting the reconfigured data to the management system.

7. The method of claim **6**, further comprising providing a translator for reconfiguring said data and transmitting said reconfigured data to the management system.

8. The method of claim **6**, wherein transmitting the reconfigured data to the management system includes transmitting the reconfigured data to a hotel property management system.

9. The method of claim **6**, further comprising storing said reconfigured data at the management system, wherein at least some of said reconfigured data is accessible by said user.

10. A system for integrating a gateway device with a management billing system, wherein the billing system can activate communication with the gateway device, comprising:

a computer;

a network gateway device in communication with said computer for connecting the computer to the computer network, wherein the network gateway device communicates with the computer absent additional agents implemented by the computer and wherein the network gateway device maintains data representative of the user's physical location and the user's access to the computer network; and

a management billing system connected to said network gateway device, wherein the management system receives the data representative of the user's access to the computer network, and wherein the management system initiates communication with the gateway device to control a user's access to the computer network and a physical location's access to the computer network.

11. The system of claim **10**, wherein the management system communicates with the network gateway device in at least one predetermined protocol selected from the group consisting of a low level protocol, a call accounting record, and a private branch telephone system protocol.

12. The system of claim **10**, wherein said management system is a hotel property management system.

13. A system for integrating a gateway device with a management system to automatically bill a user for access to a computer network, comprising:

a computer;

a network gateway device in communication with said computer for connecting the computer to the computer network, wherein the network gateway device communicates with the computer absent additional agents implemented by the computer and wherein the network gateway device maintains data representative of the user's physical location and usage of the computer network; and

a management system connected to said network gateway device for automatically billing the user based upon the physical location of the user and the usage of the computer network, wherein said management system is configured to communicate according to at least one predetermined protocol,

wherein the network gateway device formats the data to meet one of the predetermined protocols supported by said management system, and wherein said management system receives the data formatted by the network gateway device and utilizes the data formatted by the network gateway device, including the physical location of the user and the user's network usage, for billing purposes.

14. The system of claim **13**, further comprising a translator in communication with the gateway device and management system for receiving the data reconfigured by the network gateway device, said translator adapted to further reconfigure the reconfigured data, and to transmit the further reconfigured data to the management system.

15. The system of claim **13**, wherein the at least one predetermined protocol is selected from the group consisting of a low level protocol, a call accounting record, and a private branch telephone system protocol.

16. The system of claim **13**, wherein said management system is a hotel property management system.

17. The system of claim **13**, wherein the management system stores data reconfigured by the network gateway device, and wherein at least some of said data is accessible by the computer.

18. A method for integrating a gateway device with a management system to automatically bill a customer for access to a computer network, comprising:

enabling a user to access, via a network gateway device, a computer network, absent additional agents implemented by a user's computer;

collecting data corresponding to the user's access to said computer network, including a physical location of the user and the user's network usage, in said network gateway device;

reconfiguring said data to one of the predetermined data formats which may be received by a management system; and

transmitting the reconfigured data to the management system.

19. The method of claim **18**, further comprising providing a translator for reconfiguring said data and transmitting said reconfigured data to the management system.

20. The method of claim **18**, wherein reconfiguring said data comprises reconfiguring said data to one of said predetermined formats selected from the group consisting of a low level protocol, a call accounting record, and a private branch telephone system protocol.

21. The method of claim **18**, wherein transmitting the reconfigured data to the management system includes transmitting the reconfigured data to a hotel property management system.

* * * * *

US006789110B1

(12) **United States Patent**
Short et al.

(10) **Patent No.: US 6,789,110 B1**
(45) **Date of Patent: Sep. 7, 2004**

(54) **INFORMATION AND CONTROL CONSOLE FOR USE WITH A NETWORK GATEWAY INTERFACE**

(75) Inventors: **Joel E. Short**, Los Angeles, CA (US); **Barry R. Robbins**, San Diego, CA (US); **Josh J. Goldstein**, Agora Hills, CA (US); **Andrew P. Wandler**, Acton, CA (US)

(73) Assignee: **Nomadix, Inc.**, Westlake Village, CA (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

(21) Appl. No.: **09/541,877**

(22) Filed: **Apr. 3, 2000**

Related U.S. Application Data

(60) Provisional application No. 60/161,139, filed on Oct. 22, 1999.

(51) **Int. Cl.**[7] **G06F 15/177**
(52) **U.S. Cl.** **709/221**; 709/227
(58) **Field of Search** 709/203, 208, 709/221, 222, 226–228

(56) **References Cited**

U.S. PATENT DOCUMENTS

6,047,051	A *	4/2000	Ginzboorg et al.	379/130
6,085,247	A *	7/2000	Parsons et al.	709/227
6,157,946	A	12/2000	Itakura et al.	
6,286,039	B1 *	9/2001	Van Horne et al.	709/221
6,427,174	B1 *	7/2002	Sitaraman et al.	709/245
6,513,060	B1 *	1/2003	Nixon et al.	709/203
6,539,431	B1 *	3/2003	Sitaraman et al.	709/226
2001/0047392	A1 *	11/2001	Murphy, Jr. et al.	709/208
2002/0152311	A1 *	10/2002	Veltman et al.	709/227
2003/0061619	A1 *	3/2003	Giammaressi	725/95

FOREIGN PATENT DOCUMENTS

WO	WO 99/65183 A2	12/1999	

OTHER PUBLICATIONS

PCT International Search Report dated Jun. 15, 2001 for International Application No. PCT/US 00 28541, filed Oct. 16, 2000; Applicant—Nomadix, Inc., et al.

R. J. Edell, et al.; "*Billing Users and Pricing for TCP*," IEEE Journal on Selected Areas in Communications vol. 13 (1995) Sep., No. 7, New York, NY.

N. Fujino, et al.; "*Mobile Information Service Based on Multi–Agent Architecture*," IEICE Transactions on Communications, J.P. Institute Electronics Information and Comm., Eng., Tokyo, vol. E80–B, Oct., 1997.

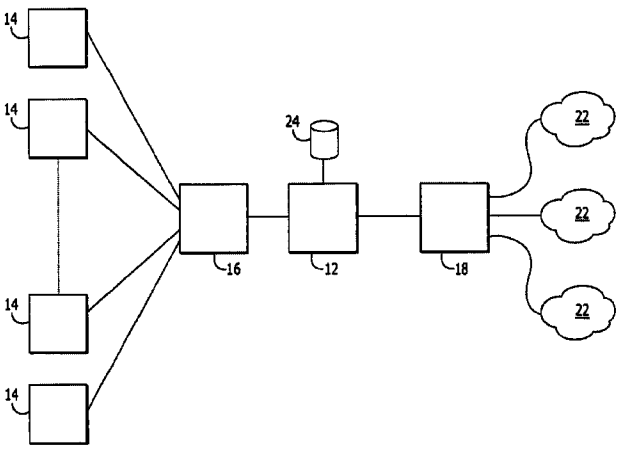
* cited by examiner

Primary Examiner—Hosain Alam
Assistant Examiner—Canh Duong
(74) *Attorney, Agent, or Firm*—Alston & Bird LLP

(57) **ABSTRACT**

A method for communicating to a host information during an existing networking session. The method comprises the steps of establishing computer network access to a user's host through a gateway interface, creating information and control console packets at the gateway interface, sending the information and control console packets to the user's host, and generating an information and control console on the monitor of the user's host that comprises data. The data will typically comprise user-specific data based upon a user's profile, the chosen billing scheme, the chosen service level or the location from which the user desires access. The gateway interface is capable of transparently connecting the user/subscriber to multiple networks without the need to reconfigure the user's host computer. The information and control console allows the gateway administrator to provide information to the user/subscriber. The information and control console may include information relating to marketing, advertising, services offered and network session monitoring parameters and the like. In one embodiment the information provided for in the information and control console may comprise network session specific data. The user/subscriber can then act on the data provided to dynamically change the features of a current network session.

36 Claims, 6 Drawing Sheets



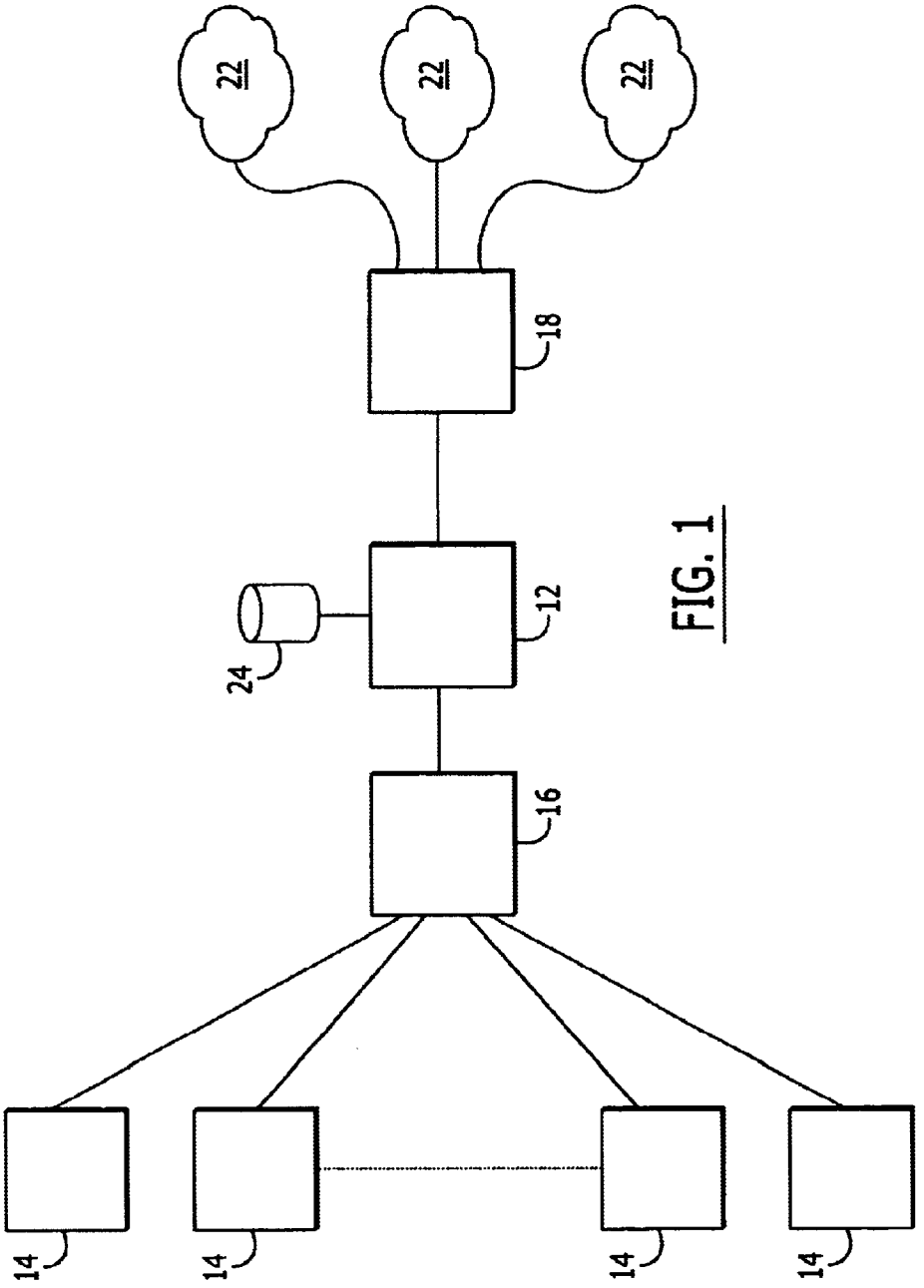


FIG. 1

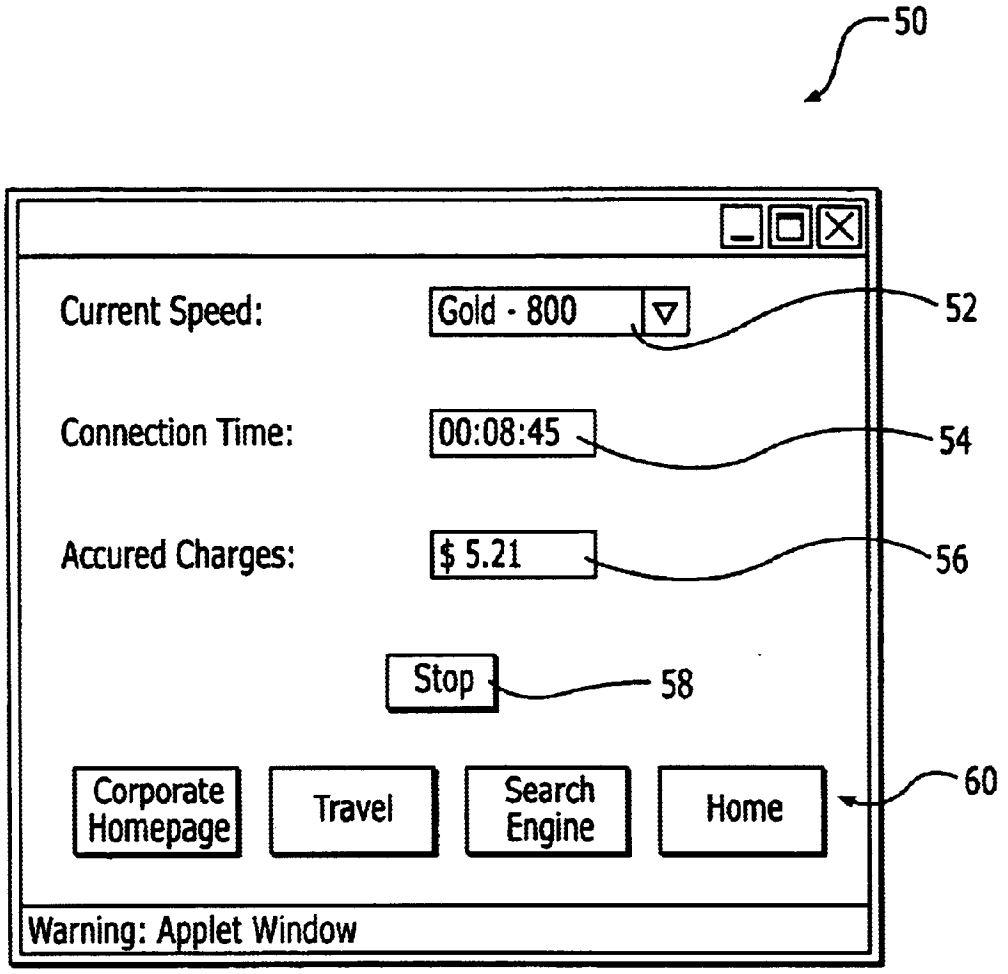

50
Current Speed:
Gold - 800
52
Connection Time:
00:08:45
54
Accured Charges:
$ 5.21
56
Stop
58
Corporate Homepage
Travel
Search Engine
Home
60
Warning: Applet Window

FIG. 2

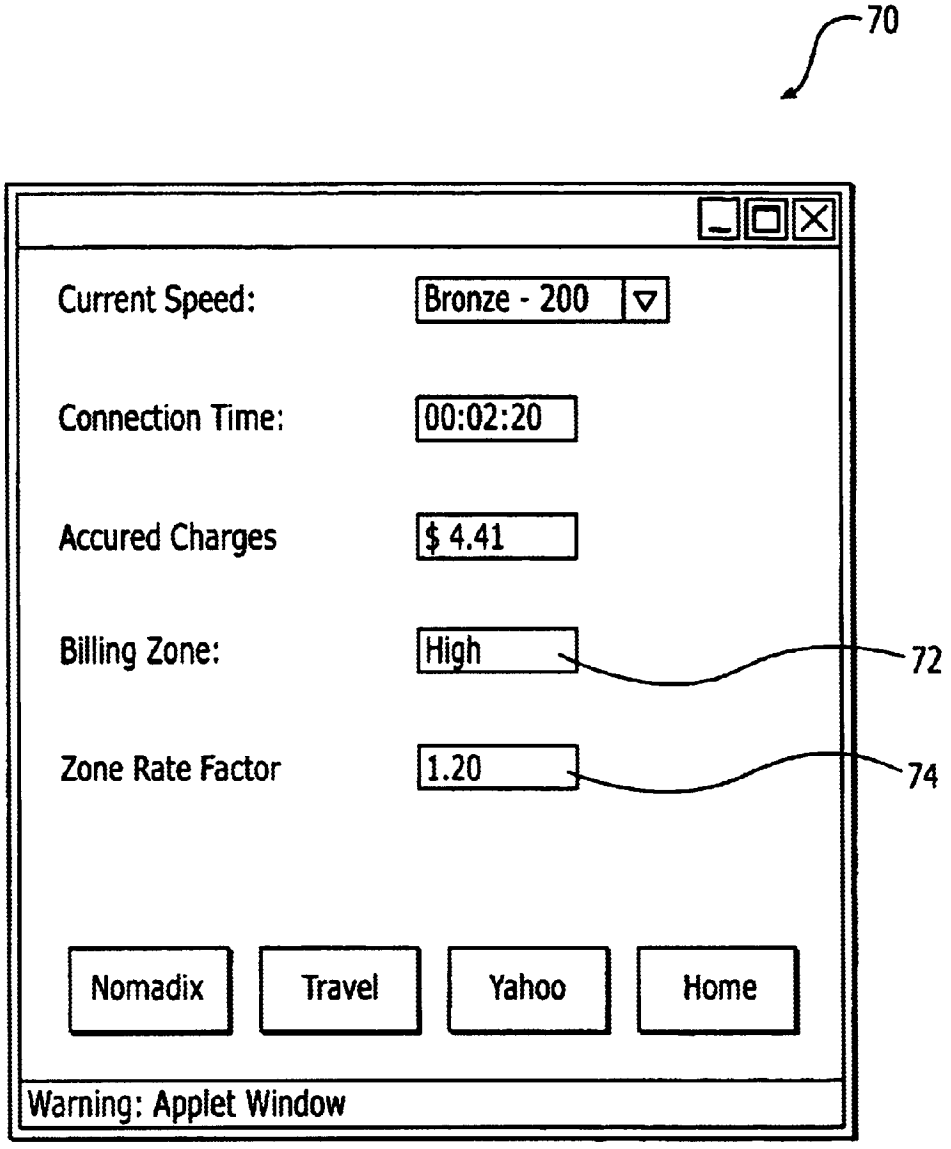

70
Current Speed:
Bronze - 200
Connection Time:
00:02:20
Accured Charges
$ 4.41
Billing Zone:
High
72
Zone Rate Factor
1.20
74
Nomadix
Travel
Yahoo
Home
Warning: Applet Window

FIG. 3

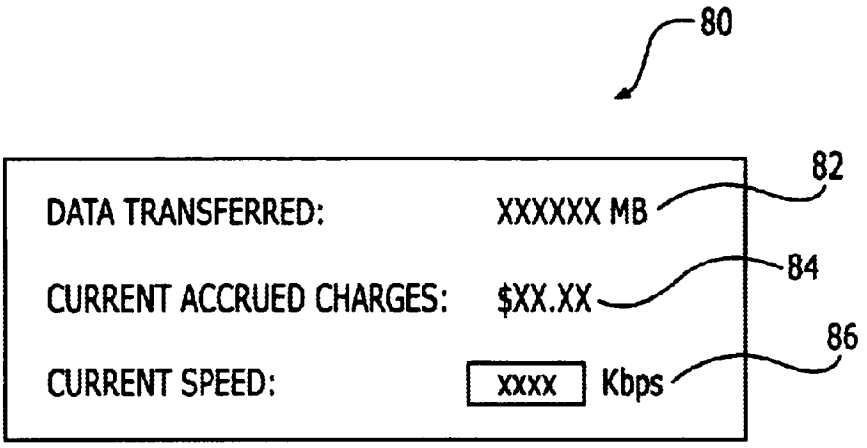

80
82
DATA TRANSFERRED:
XXXXXX MB
84
CURRENT ACCRUED CHARGES:
$XX.XX
86
CURRENT SPEED:
xxxx
Kbps

FIG. 4

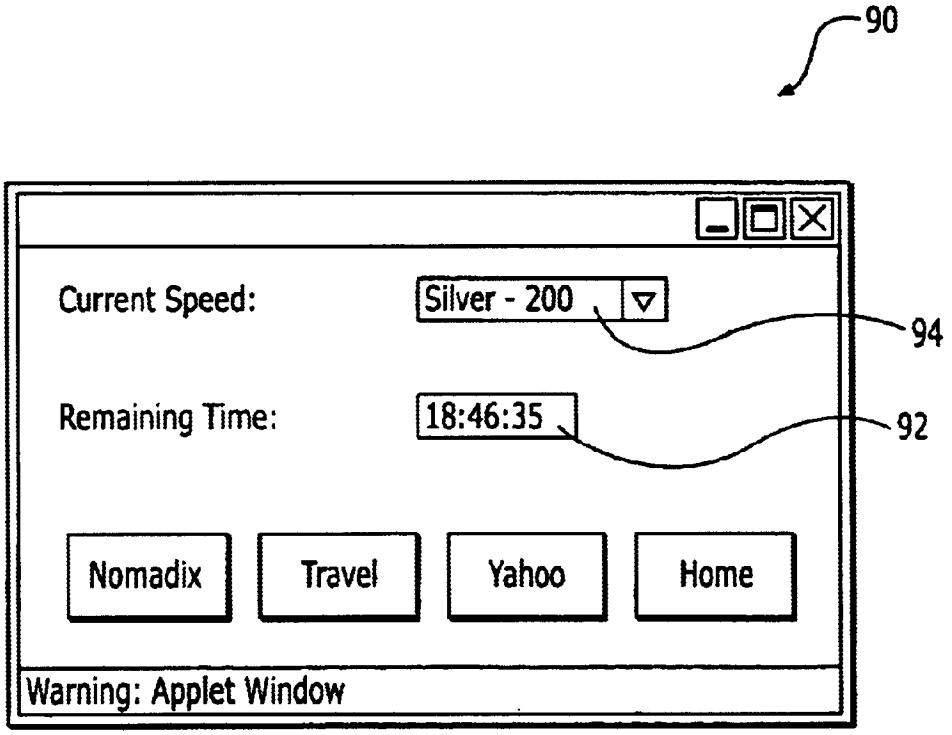

90
Current Speed:
Silver - 200
94
Remaining Time:
18:46:35
92
Nomadix
Travel
Yahoo
Home
Warning: Applet Window

FIG. 5

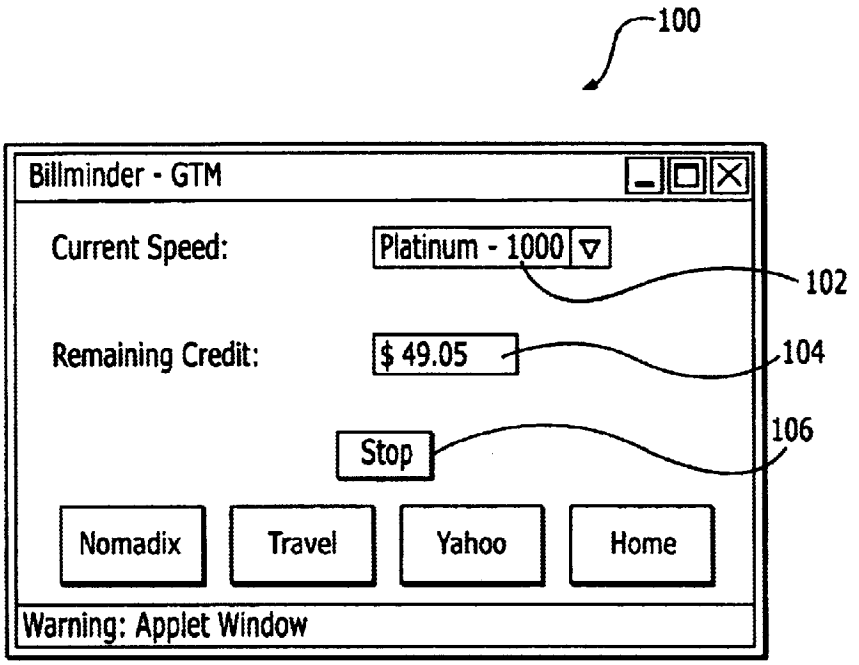

100
Billminder - GTM
Current Speed:
Platinum - 1000
102
Remaining Credit:
$ 49.05
104
Stop
106
Nomadix
Travel
Yahoo
Home
Warning: Applet Window

FIG. 6

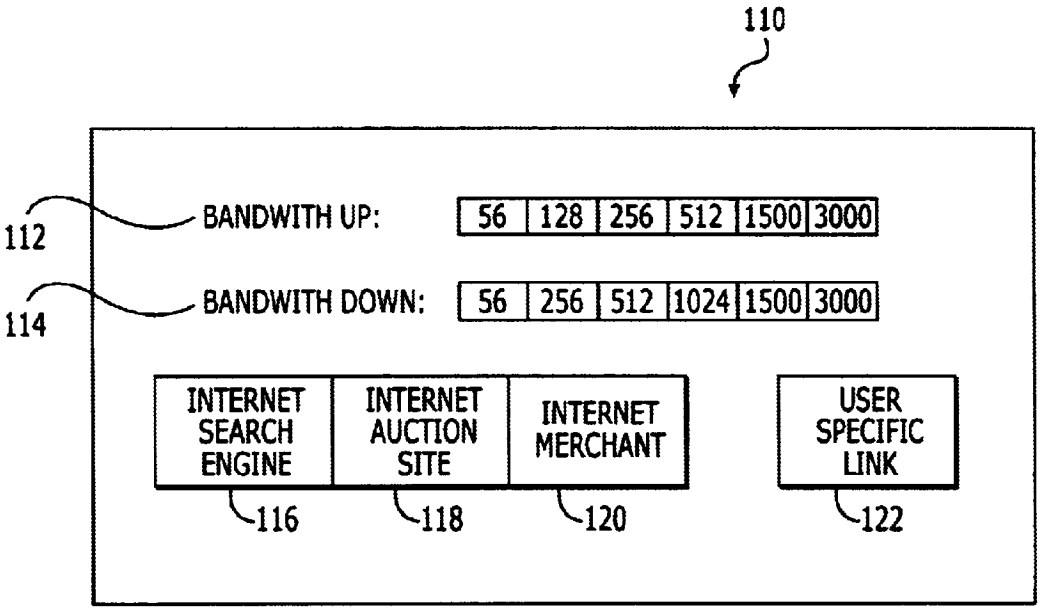

110
112
BANDWITH UP:
56 128 256 512 1500 3000
114
BANDWITH DOWN:
56 256 512 1024 1500 3000
INTERNET SEARCH ENGINE
INTERNET AUCTION SITE
INTERNET MERCHANT
USER SPECIFIC LINK
116
118
120
122

FIG. 7

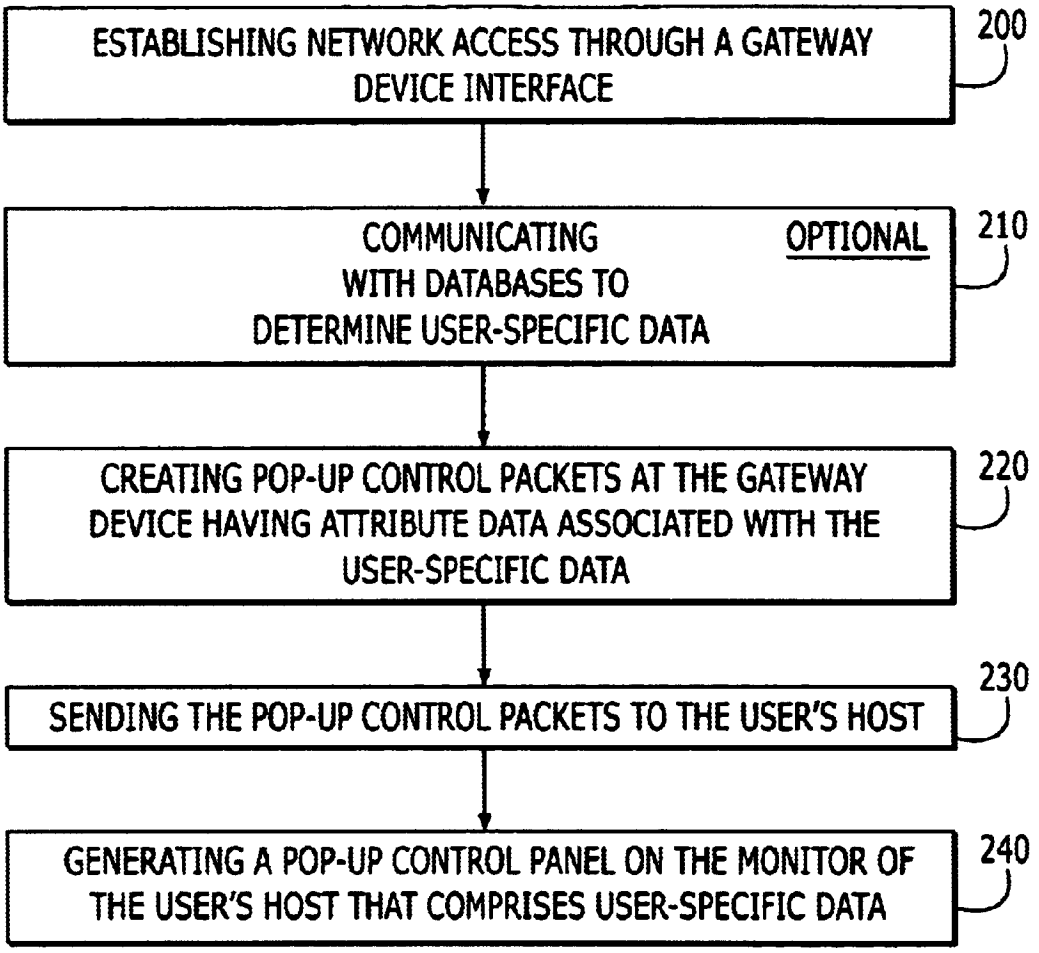

ESTABLISHING NETWORK ACCESS THROUGH A GATEWAY DEVICE INTERFACE
200
COMMUNICATING WITH DATABASES TO DETERMINE USER-SPECIFIC DATA
OPTIONAL
210
CREATING POP-UP CONTROL PACKETS AT THE GATEWAY DEVICE HAVING ATTRIBUTE DATA ASSOCIATED WITH THE USER-SPECIFIC DATA
220
SENDING THE POP-UP CONTROL PACKETS TO THE USER'S HOST
230
GENERATING A POP-UP CONTROL PANEL ON THE MONITOR OF THE USER'S HOST THAT COMPRISES USER-SPECIFIC DATA
240

FIG. 8

INFORMATION AND CONTROL CONSOLE FOR USE WITH A NETWORK GATEWAY INTERFACE

CROSS-REFERENCE TO RELATED APPLICATIONS

The present application claims priority from U.S. Provisional Patent Application Serial No. 60/161,139, the contents of which are incorporated by reference.

FIELD OF THE INVENTION

The present invention relates generally to a network gateway interface and, more particularly, to an information and control console for use with a network gateway interface.

BACKGROUND OF THE INVENTION

In order for a computer to function properly in a network environment, the computer must be appropriately configured. Among other things, this configuration process establishes the protocol and other parameters by which the computer transmits and receives data. In one common example, a plurality of computers are networked to create a local area network (LAN). In the LAN, each computer must be appropriately configured in order to exchange data over the network. Since most networks are customized to meet a unique set of requirements, computers that are part of different networks are generally configured in different manners in order to appropriately communicate with their respective networks.

While desktop computers generally remain a part of the same network for a substantial period of time, laptops, handhelds, personal digital assistants (PDAs), cellphones or other portable computers (collectively "portable computers") are specifically designed to be transportable. As such, portable computers are connected to different networks at different times depending upon the location of the computer. In a common example in which the portable computer serves as an employee's desktop computer, the portable computer is configured to communicate with their employer's network, i.e., the enterprise network. When the employee travels, however, the portable computer may be connected to different networks that communicate in different manners. In this regard, the employee may connect the portable computer to the network maintained by an airport, a hotel, a cellular telephone network operator or any other locale in order to access the enterprise network, the Internet or some other on-line service. The portable computer is also commonly brought to the employee's residence where it is used to access various networks, such as, the enterprise network, a home network, the Internet and the like. Since these other networks are configured somewhat differently, however, the portable computer must also be reconfigured in order to properly communicate with these other networks. Typically, this configuration is performed by the user each time that the portable computer is connected to a different network. As will be apparent, this repeated reconfiguration of the portable computer is not only quite time consuming, but is also prone to errors. The reconfiguration procedure may even be beyond the capabilities of many users or in violation of their employer's information technology (IT) policy.

As described by U.S. patent applications Ser. No. 08/816,174 entitled "Nomadic Router", filed on Mar. 12, 1997, and now abandoned in the name of inventors Short et. al., and

U.S. patent application Ser. No. 09/458,602 entitled "Systems and Methods for Authorizing, Authenticating and Accounting Users Having Transparent Computer Access to a Network Using a Gateway Interface", filed on Dec. 08, 1999, and still pending in the name of inventors Pagan, et. al., a Universal Subscriber Gateway (USG) device has been developed by Nomadix, Inc. of Westlake Village, Calif., the assignee of the present invention. The contents of both of these applications are expressly incorporated by reference as if fully set forth herein. The gateway interface serves as an interface connecting the user/subscriber to a number of networks or other online services. For example, the gateway interface can serve as a gateway to the Internet, the enterprise network, or other networks and/or on-line services. In addition to serving as a gateway, the gateway interface automatically adapts to a host, in order that it may communicate with the new network in a manner that is transparent both to the user/subscriber and the new network. Once the gateway interface has appropriately adapted to the user's host, the host can communicate via the new network, such as the network at a hotel, at home, at an airport, or any other location, in order to access other networks, such as the enterprise network, or other online services, such as the internet.

The transient user/subscriber, and more specifically the remote or laptop user, benefits from being able to access a myriad of computer networks without having to undergo the time-consuming and all-too-often daunting task of reconfiguring their host in accordance with network specific configurations. From another perspective, the network service provider benefits from avoiding "on-site" visits and/or technical support calls from the user who is unable to properly re-configure the portable computer. In this fashion, the gateway interface is capable of providing more efficient network access and network maintenance to the user/subscriber and the network operator.

A gateway interface is also instrumental in providing the user/subscriber broadband network access that can be tailored to the user's needs. In many instances the remote user is concerned with being able to acquire network access and levels of service in the most cost-effective manner. Correspondingly, the gateway interface administrator desires the capability to be able to offer the user/subscriber numerous different service, routing, and billing rate options. By way of example, the remote user in a hotel environment may desire a network subscription for the duration of their hotel stay while the user in an airport may desire a network subscription for the duration of their layover or until their scheduled flight departs. Additionally, a user may desire a certain level of service based on bandwidth concerns and the need for higher or lower data transfer rates. For example, the user/subscriber who is accessing a network for the purpose of viewing text may desire a lower bandwidth service level that meets their particular needs, however, another user/subscriber who is accessing a network for the purpose of downloading files may desire a higher bandwidth service level capable of transferring data at higher speeds.

Additionally, the network service provider benefits from being able to offer various service, routing and billing options to the user/subscriber. By offering service at varying speeds and pricing scales, the network service provider is able to minimize network congestion, i.e. not all user/subscribers are tied to one high speed (and high cost) service. Lessening network traffic is beneficial for attracting new subscribers and insuring that pre-existing subscribers maintain status quo. From an economic standpoint, differentiated service quality and usage based pricing will pro-

mote the use and deployment of broadband network access and enhance the revenue models of the network service providers. No longer will the user/subscriber be tied to a flat-rate billing scheme that offers a single level of service quality. Flat-rate pricing and single level service quality consumes resources, requires light network users to subsidize heavy users, and hinders the dissemination of widespread use of broadband network access. Additionally, the ability to provide differentiated service quality and usage based pricing can be enhanced by providing these features on demand and dynamically throughout the user's network session. For a more detailed discussion of the need to provide differentiated quality of service and billing schemes to the broadband network environment see "Providing Internet Access: What We Learn From INDEX", INDEX project report #99-010W, Apr. 16, 1999, (http://www.INDEX.Berkeley.edu/reports/99-010W), R. J. Edell et.al. That document is herein expressly incorporated by reference as if setforth fully herein.

In today's fast paced computing and networking environment it is even more advantageous to provide these service and billing options dynamically, allowing the user/subscriber to change, for example, billing rates, service routing or bandwidth capacity while a network session is on going. This would allow the user/subscriber to be billed at one rate while downloading the data-intensive file while choosing a more cost-effective billing structure for the less data-intensive activities. Additionally, the dynamic nature of this process would allow the user/subscriber to change service levels or billing rates without the need to exit the network and initiate a new log-on procedure. In effect, the user/subscriber benefits from having a more efficient and less time-consuming means of altering service levels and billing structure.

In order to make the user/subscriber constantly aware that these diverse service and billing options exist the gateway interface administrator needs to be able to provide the user/subscriber with real-time information pertaining to the network session(s) that the user currently has on-going. The gateway administrator would benefit from being able to provide the user/subscriber with constant or intermittent data related to the network sessions currently on-going, the duration of those sessions, the bandwidth currently being used, the number of bytes that have been transferred and any other information related to the current network session. In this manner, the user/subscriber has the capability to monitor and make the appropriate adjustments to the billing structure and/or service levels related to the network sessions that he or she currently has on going. The user/subscriber may choose to stop or shutdown connections (and thus billing) to those networks not currently being utilized. The user/subscriber may monitor the duration of the network session and determine that a longer subscription is necessary or the user may observe the bandwidth currently used and determine that the current application warrants an increase or decrease in bandwidth. The ability to provide this real-time information to the user is especially important in light of the fact that the typical, infrequent gateway interface user will be unfamiliar with billing and service structure and, particularly, the capability to change these features on-the-fly.

From the perspective of the network service provider, the ability to offer flexible service quality, routing options and billing plans ultimately can lead to less overall network congestion. The current broadband standard of flat rate billing and one-dimensional service and routing options force the network service provider in to effectively transmitting all network data at maximum bandwidth. By lessening the congestion within the network, the service provider is able to accommodate more user/subscribers and provide those user/subscribers with a more effective network. The ability to lessen congestion is even more apparent if the network service provider can offer the user/subscriber the capability to make changes to the service quality, routing and billing structure while the network session is on going. Additionally, by offering differentiated quality of service, routing and billing the network service provider may be able to increase the volume of user/subscribers accessing the network.

SUMMARY OF THE INVENTION

The present invention comprises an information and control console that is administered through a gateway interface. The gateway interface is capable of transparently connecting the user/subscriber to multiple networks without the need to reconfigure the user's host computer. The information and control console allows the gateway administrator, the Internet service provider (ISP) and/or application service provider (ASP) to provide real-time information to the user/subscriber. The information provided to the user in the information and control console may be user-specific information related to the current network session, the current location of the user's host, user-specific profile type information or the like. The user/subscriber can then act on the data provided to dynamically change the features of a current network session. Additionally, the information and control console can provide for information or access to information through appropriate links. In many instances, the information provided or the links to information may be user-specific information. The basis or "know-how" for the user-specific data can be provided by the network service provider (i.e. user profiles in the network database) or through direct user inputs.

The information and control console provides the gateway administrator, the ISP and/or the ASP the capability to provide the user with limitless forms of information and networking options. For example, the gateway administrator can provide the user with network session monitoring information, or it can provide for marketing capabilities through advertising medium or it can provide the gateway administrator with a means to poll or survey users. The ISP and/or the ASP can provide the user with user-specific targeted marketing and advertising information or various service delivery platforms. These examples of the types of information that an information and control console may provide should not be construed as limiting. The information and control console may be configured by the gateway administrator, network provider or user/subscriber to provide a wide variety of information.

In one embodiment of the invention an information and control console is provided to a user/subscriber during a network session. The information and control console may include information and links to information in response to configuration of the panel by the gateway administrator or the subscriber/user. In many instances, the information that is provided for in the information and control console will be user-specific data assembled from user profiles in network databases or from direct user/subscriber inputs. The information that is provided to the user/subscriber via the information and control console may include monitoring of the network session, polling/surveying the user/subscriber, user-tailored advertisements and information on other services/features offered by the gateway administrator, the network provider and/or the application service provider.

In another embodiment of the present invention the information and control console may include network monitoring attributes such as, identifying the network session(s) currently in-use, identifying the duration of network sessions currently in-use, identifying the bandwidth currently available for a specific network session and identifying the current amount of bytes received and/or sent for a specific network session. It is to be understood, by those skilled in the art to which this invention relates that all conceivable useful information relating to the current network session could be displayed to the user/subscriber in a multitude of combinations as defined by the user/subscriber and/or the gateway administrator. The gateway administrator will have the capability to dynamically change the information supplied in the information and control console based on many factors, including the location of the user/subscriber, the profile of the user/subscriber and the chosen billing scheme and service level.

In yet another embodiment of the present invention a method is provided for communicating to a network user predefined information during an ongoing networking session. The method comprises of the steps of establishing computer network access to a user s host through a gateway interface that has the capacity to transparently configure a host to meet the requirements of available networks. In one embodiment, after the gateway interface has granted access to the host the gateway interface communicates with databases associated with the gateway interface to determine user-specific data. The user-specific data may include user-profiled information, host-location-related data, user-specific network monitoring information or the like. This user-specific data is then used to create information and control console packets at the gateway interface, which are then sent to the user's host. The information and control console packets reach the host and generate information and control consoles on a monitor of the user's host. The information and control consoles will comprise data that typically is related to a user's profile, the chosen billing scheme, the chosen service level, the location from which the user desires access or any other information deemed pertinent by the gateway administrator or user/subscriber.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. **1** is a block diagram of a computer system that includes a gateway interface for automatically configuring one or more computers to communicate via the gateway interface with other networks or other online services.

FIGS. **2–7** are illustrations of various examples of information and control consoles, in accordance with an embodiment of the present invention.

FIG. **8** is a flowchart diagram of a method for communicating to a network user data during an ongoing network session, in accordance with an embodiment of the present invention.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

The present invention now will be described more fully hereinafter with reference to the accompanying drawings, in which preferred embodiments of the invention are shown. This invention may, however, be embodied in many different forms and should not be construed as limited to the embodiments set forth herein; rather, these embodiments are provided so that this disclosure will be thorough and complete, and will fully convey the scope of the invention to those skilled in the art. Like numbers refer to like elements throughout.

Referring now to FIG. **1**, the computer network system **10** that includes a gateway interface **12** is depicted in block diagram form. The computer network system typically includes a plurality of hosts **14** that access the computer network system in order to gain access to other networks or other online services. For example, the hosts can be plugged into ports that are located in different rooms of a hotel or a multi-dwelling residence. Alternatively, the hosts can be plugged into ports in an airport, an arena, or the like. The computer network system includes a gateway interface that provides for an access point between the plurality of computers and the various networks or other online services. Most commonly, the gateway interface is located near the hosts at a relatively low position in the structure of the overall network. (i.e. the gateway interface will be located within the hotel, multi-unit residence, airport, etc.) However, the gateway interface can be located at a higher position in the overall network structure such as at a Point of Presence (PoP) within a Network Operating Center (NOC), if so desired. Although the gateway interface can be physically embodied in many different fashions, the gateway interface typically includes a controller and a memory device in which software is stored that defines the operational characteristics of the gateway interface. Alternatively, the gateway interface can be embedded within another network device, such as the access controller or a router, or the software that defines the functioning of the gateway interface can be stored on a PCMCIA card that can be inserted into the computer in order to automatically reconfigure the computer to communicate with a different computer system.

The computer network system **10** also typically includes an access controller **16** positioned between the hosts **14** and the gateway interface **12** for multiplexing the signals received from the plurality of computers onto a link to the gateway interface. Depending upon the medium by which the hosts are connected to the access controller, the access controller can be configured in different manners. For example, the access controller can be a digital subscriber line access module (DSLAM) for signals transmitted via regular telephone lines, a cable head end for signals transmitted via coaxial cables, a wireless access point (WAP) for signals transmitted via a wireless network, a cable modem termination system (CMPS), a switch or the like. As also shown in FIG. **1**, the computer system typically includes one or more routers **18** and/or servers (not shown in FIG. **1**) of a plurality of computer networks **20** or other online services **22**. While the computer system is depicted to have a single router, the computer system can have a plurality of routers, switches, bridges, or the like that are arranged in some hierarchical fashion in order to appropriately route traffic to and from the various networks or other online services. In this regard, the gateway interface typically establishes a link with one or more routers. The routers, in turn, establish links with the servers of other networks or other online service providers, such as internet service providers, based upon the subscriber's selection.

The gateway interface **12** is specifically designed to adapt to the configuration of each of the hosts **14** that log onto the computer network system **10** in a manner that is transparent to the subscriber and the computer network. In the typical computer network that employs dynamic host configuration protocol (DHCP) service, an IP address is assigned to the computer that is logging onto the computer network through communication with the gateway interface. The DHCP service can be provided by an external DHCP server **24** or it can be provided by an internal DHCP server located in unison with the gateway interface. Upon opening their web

browser or otherwise attempting to access an on-line service, the gateway interface will direct the subscriber to enter some form of an identifier such as their ID and password. In an alternate embodiment of the device, it is anticipated that the gateway interface will be able to automatically detect this information upon connection of the computer to the network or any attempt to log in. The gateway interface then determines if the subscriber is entitled to access the computer system, the level of access and/or the type of services to which the subscriber is entitled according to an Authentication, Authorization and Accounting (AAA) procedure. For a more detailed discussion of the AAA procedure see U.S. patent application Ser. No. 08/816,174 and U.S. patent application Ser. No. 09/458,602, both applications have been assigned to Nomadix, L.L.C., the assignee of the present invention and have been previously incorporated by reference as if setforth fully herein. An AAA server, which is a database of subscriber records, may be remote to the gateway interface or the AAA database may be incorporated into the physical embodiment housing the gateway interface. Assuming that the subscriber has been authenticated and has authorization, the gateway interface typically presents new subscribers with a home page or control panel that identifies, among other things, the online services or other computer networks that are accessible via the gateway interface. In addition, the home page presented by the gateway interface can provide information regarding the current parameters or settings that will govern the access provided to the particular subscriber. As such, the gateway administrator can readily alter the parameters or other settings in order to tailor the service according to their particular application. Typically, changes in the parameters or other settings that will potentially utilize additional resources of the computer network system will come at a cost, such that the gateway administrator will charge the subscriber a higher rate for their service. For example, a subscriber may elect to increase the transfer rate at which signals are transmitted across the computer network and pay a correspondingly higher price for the expedited service.

The home page also permits the subscriber to select the computer network **20** or other online services **22** that the subscriber wishes to access. For example, the subscriber can access the enterprise network on which the computer is typically resident. Alternatively, the subscriber can access the internet or other on-line services. Once the subscriber elects to access a computer network or other online service, the gateway interface establishes an appropriate link via one or more routers **18** to the desired computer network or online service.

Thereafter, the subscriber can communicate freely with the desired computer network **20** or other online service **22**. In order to support this communication, the gateway interface **12** generally performs a packet translation function that is transparent to the user/subscriber and the network. In this regard, for outbound traffic from the computer **12** to the computer network or other on-line service, the gateway interface changes attributes within the packet coming from the user/subscriber, such as the source address, checksum, and application specific parameters, to meet the criteria of the network to which the user/subscriber has accessed. In addition, the outgoing packet includes an attribute that will direct all incoming packets from the accessed network to be routed through the gateway interface. In contrast, the inbound traffic from the computer network or other online service that is routed through the gateway interface, undergoes a translation function at the gateway interface so that the packets are properly formatted for the user/subscriber's host. In this manner, the packet translation process that takes place at the gateway interface is transparent to the host, which appears to send and receive data directly from the accessed computer network. Additional information regarding the translation function is provided by U.S. patent application Ser. No. 08/816,714, assigned to Nomadix L.L.C, the assignee of the present invention and previously incorporated by reference as if setforth herein. By implementing the gateway interface as an intermediary between the user/subscriber and the computer network or other online service, the user/subscriber will eliminate the need to re-configure their host **12** upon accessing subsequent networks.

In one embodiment of the present invention, the gateway interface implements an information and control console. Once the user/subscriber has gained access to one or more networks through the gateway interface the information and control console is communicated to the host computer from the gateway interface and provides the user/subscriber with information. The information that is provided to the user/subscriber in the information and control console may include information of various types, forms and content. The information that is provided for in the information and control console may be static information or dynamic information. The information provided in the information and control console may be user specific, site specific or gateway interface specific. In the user-specific model the data may be based on information found in network databases or information provided by the user/subscriber. For example, the network databases may include user profiles that have been assembled by querying the user or by logging the networks and sites visited by the user. Additionally, the information provided for in the information and control console may be network monitoring information, for marketing purposes or any other conceivable purpose that the gateway administrator or user/subscriber deems appropriate.

Within the realm of marketing, the information and control console may include advertising tailored to the specific needs of the user/subscriber. The gateway interface would be capable of tailoring the information based upon the current location of the user s host, user profiles in the network, gateway administrator concerns or the like. Typically, this information is provided for in the information and control console in the form of links to other available networks, Internet sites, intranets or similar networking possibilities. In this fashion, the gateway administrator can offer the user/subscriber access to other networks and services without the user/subscriber having to register for or be approved for a subscription to these other networks or services. The gateway administrator can act as a broker for these other networks and services and, thereby, offer the user/subscriber short-term access to these networks and services at reduced rates.

The information and control console may also incorporate surveys or links to surveys to provide the gateway administrator or network provider with beneficial statistical data. As an ancillary benefit, the user/subscriber who responds to the surveys may be rewarded with network access credit or upgraded quality. Additionally, the gateway administrator can offer additional services to the user/subscriber by way of the information and control console or links to these services may be offered on the information and control console. These services offered by the network service provider are not limited to the services related to the network connection. For example, a hotel may desire to offer the user/subscriber in-room food service or a multi-unit dwelling may want to offer house cleaning service.

The information and control console may also comprise network monitoring information related to the status of the current network session. By way of example this information may include, current billing structure data, the category/level of service that the user/subscriber has chosen, the bandwidth being provided to the user, the bytes of information currently sent or received, the current status of network connection(s) and the duration of the existing network connection(s). It is to be understood, by those skilled in the art to which this invention relates that all conceivable useful information relating to the current network session could be displayed to the user/subscriber in a multitude of combinations as defined by the user/subscriber and/or the gateway administrator. The gateway administrator will have the capability to dynamically change the information supplied in the information and control console based on many factors, including the location of the user/subscriber, the profile of the user subscriber and the chosen billing scheme and service level. The information provided in the information and control console may prompt the user/subscriber to return to the provisioning page to adjust any number of specific parameters, such as the billing scheme, the routing, the level of service and/or other user-related parameters or the user may be able to adjust the billing scheme and service level by responding directly to the information and control console.

The information and control console may be implemented with an object-oriented programming language such as Java developed by Sun Microsystems, Incorporated of Mountain View, Calif. The code that defines the information and control console is embodied within the gateway interface, while the display monitor and the driver are located with the host computer's that are in communication with the gateway interface. The object oriented programming language that is used should be capable of creating executable content (i.e. self-running applications) that can be easily distributed through networking environments. The object oriented programming language should be capable of creating special programs, typically referred to as applets that can be incorporated in web pages to make them interactive. In this invention the applets take the form of the information and control consoles. It should be noted that the chosen object-oriented programming language would require that a compatible web browser be implemented to interpret and run the information and control console. It is also possible to implement the information and control console using other programming languages, such as HTML; however, these languages may not be able to provide all the dynamic capabilities that languages, such as Java provide.

The gateway administrator or the user/subscriber may have control over how frequently an information and control console is invoked by the gateway interface so that it appears on the monitor of the user/subscriber. Typically the gateway interface will be configured to invoke an initial information and control console to the user/subscriber's host a short period of time after the user has gained access to a network service provided by the gateway administrator. Additionally, the information and control console may be invoked automatically in response to predetermined conditions. An example being, invoking the information and control console in response to the user/subscriber's imminent subscription expiration. The information and control console may also be generated and controlled by the user/subscriber. The user/subscriber can choose to have the information and control console visual throughout the network session or the pop-up control can be minimized or deleted. It is also possible for the gateway administer to configure the information and control console so that it can not be deleted or the user/ subscriber can be rewarded (e.g. additional access time or the like) for maintaining a visible pop-up control throughout the network session.

The information and control console is configured to send heartbeat packets back to the gateway interface at predetermined specified intervals to let the gateway know that the user/subscriber still has an active, information and control console in use or at the user's disposal. If the gateway interface does not receive a heartbeat from the host after a predetermined period of time, it will assume that the user has deleted the information and control console or the information and control console has otherwise failed. In the instance where a heartbeat is not received by the gateway interface after a predetermined time period, the gateway interface will re-send a new updated information and control console to the user/subscriber. Through the use of these "heartbeats" the gateway interface will be able to insure that the user/subscriber always has ready access to the user-related information provided by the information and control console. The user/subscriber will also have the capability to locate the information and control console anywhere within the viewable area of the computer monitor. The physical embodiment of the information and control console can be modified in an infinite number of ways to suit either the user or the gateway administrator. For example, the panel size, color, graphics, location, form of read out (digital vs. analog), language, scales (e.g. metric vs. U.S.) can all be varied, as well as the rate at which information is provided. Additionally, the information and control console may be configured by the user or gateway administrator such that the outlining panel and background of the console are transparent and, thus, only the linking buttons and other information are visible on the monitor.

It should be noted that in most embodiments the information and control console will only be actively sent from the gateway interface if the user/subscriber is accessing a network provided service, such as broadband Internet access, that is provided by the gateway administrator. If the user chooses to stop using the network service, such as broadband Internet access, they can close the application and the information and control console will correspondingly be inactive. The gateway interface recognizes that the network provided service has been disabled and stops sending information and control console packets to the host. Upon the user/subscriber re-activating the network provided service, the gateway interface will recognize the need to send a new information and control console and begin recognizing "heartbeats" coming from the information and control console. However, it also possible to configure the gateway interface to send information and control console packets to the user/subscriber who is not currently activating a network service or currently involved in a networking session. For offline sending of information and control console packets the host must be in networking communication with the gateway interface.

FIGS. **2–6** are depictions of various examples of information and control consoles providing for network session data. These information and control consoles are shown by way of example to illustrate the various user specific information that the information and control consoles may contain. These information and control consoles are typically associated with a specific billing and/or service level plan. The gateway administrator or the network operator may choose to offer any or all of these billing and/or service options. The information and control console that will be sent to the user/subscriber's computer may be tailored to reflect the user data that is pertinent to the chosen and available billing methods and/or service levels.

FIG. **2** shows an information and control console **50**, that includes the current chosen connection speed (i.e. bandwidth) **52**, an elapsed time counter **54**, a current charges accrued counter **56** and a start/stop button **58**. The attribute fields in this information and control console are typically used if the gateway administrator or network operators offer a billing plan based on the bandwidth that the user selects, commonly referred to as a "pay-per-use" method of billing. For example, the gateway administrator or network operators may structure billing at $0.10 per minute for 200 Kbps bandwidth, $0.20 per minute for 400 Kbps bandwidth and $0.35 per minute for 800 Kbps per minute bandwidth. If the user chooses 200 Kpbs at $0.10 per minute, then the initial information and control console will identify 200 Kpbs as the current bandwidth along with the elapsed time that the user has been connected to the accessed network and a running total of the charges that have been incurred. If the user/subscriber desires to change the bandwidth setting, they can click-on the box containing the current bandwidth and are re-directed to a service provisioning screen to choose an alternative billing method.

The start/stop buttons **58** allow the user the benefit of stopping the charges to an account (i.e. temporarily disabling the network) without closing the user's web browser. A user/subscriber can activate the stop button and be re-directed back to the home page or portal page. From the user/subscriber standpoint the ability to momentarily disable the network and stop incurring charges is a cost-effective form of networking. From the gateway administrator or network operator standpoint the momentary network stoppage means the user will be directed back to the portal or home page. By re-directing the user back to the portal or home page the gateway administrator or network operator is provided the opportunity to present the user/subscriber with updated information pertaining to the remote location (i.e. the hotel, the airport etc.). When the user desires to re-establish network connection the user may activate the start button on the information and control console and charges will again incur. The start/stop buttons may be implemented at the discretion of the gateway administrator or network operator and most of the billing plans and service plans will provide for the option of presenting the start/stop button feature within the information and control console. Additionally, the information and control console may comprise a timer (not shown in FIGS. **2–6**) that alerts the user/subscriber that a subscription is about to expire.

Additional information and control console fields are provided in the form of click-on buttons **60** located, in this instance, near the bottom of the pop-up panel. By way of example the buttons shown in FIG. **2** provide for links to a corporate home page, a travel site on the Internet, an Internet search engine and a network provider home page. Those of ordinary skill in the art will note that the additional fields within the pop-up panel may encompass infinite possibilities for links, services and information. Additionally, the buttons or any other field within the information and control console may include other types of information options, such as advertising fields or user-specific links or fields based upon data found in the user's profile or inputted by the user/subscriber.

FIG. **3** depicts an information and control console **70** having the additional attribute fields of billing zone **72** and rate factor **74**. The gateway administrator or network operators may choose to charge a premium for access during peak usage periods. These periods, or zones, will typically be defined by the hours in the day or the days of the week (i.e. weekday versus weekend day). For example network usage during the 9 am to 5 pm period may be billed at a rate factor of 1.25, while network usage during the 5 pm to 9 am period may be billed at a rate factor of 1.0. Thus, the information and control console will include the billing zone that the user/subscriber currently occupies, as well as the rate factor that is tied to the specific billing zone. The user/subscriber will have been made aware of billing zones and rate factors when the initial service provisioning screen was presented during the log-on and billing process.

FIG. **4** illustrates an information and control console **80** that includes the current data transferred counter **82**, current charges accrued counter **84**, and current connection speed **86**. The attribute fields in this information and control console are typically used if the gateway administrator or network operators offers a billing plan based on the quantity of data that is transferred, typically both sent and received data, commonly referred to as a "bitmeter" method of billing. For example, the gateway administrator or network operator may choose to charge user/subscribers the flat rate of $1.00 per megabyte of data transmitted. If the user/subscriber desires to change the bandwidth setting, they can click-on the box containing the current bandwidth and are re-directed to a service provisioning screen to choose an alternative bandwidth. The start/stop buttons, not shown in FIG. **4**, may also be implemented in this information and control console.

FIG. **5** shows an information and control console **90** that includes a time remaining counter **92** and a current connection speed **94**. The attribute fields in this information and control console are typically used if the gateway administrator or network operators offer a billing plan based on a specific level of service (i.e. desired bandwidth) for a specific period of time, commonly referred to as an "expiration time" method of billing. In this billing and service scheme, the user/subscriber may choose different pricing schemes based on the level of service (i.e. desired bandwidth) and the duration of their subscription. For example, the user may be offered a 1, 2, 4, 8 or 24 hour subscription with the option to operate at a 200, 400 or 800 Kpbs bandwidth. If the user/subscriber desires to change the duration of the subscription or the level of service, it may be possible to click-on the box containing the remaining time or current bandwidth, be re-directed to a service provisioning screen and choose an alternate service plan offering a higher level of service or a longer subscription period. The start/stop buttons will not typically be employed in the "expiration time" method because the subscription has a specific time duration.

FIG. **6** illustrates an information and control console **100** that includes current connection speed **102**, a remaining credit counter **104** and a start/stop button **106**. The attribute fields in this information and control console are typically used if the gateway administrator or network operator offers a billing plan based on pre-purchasing a desired amount of network "credit". In this type of billing scheme the user/subscriber will be offered various bandwidth options, each of which is tied to specified costs per minute of use. The user will then purchase a "block" of network access, for example $20.00 of network use. The block of network access will then allow the user to choose the bandwidth of the connection. If the user chooses a slow connection speed they will deplete their "block" of network access more slowly than if they choose a higher connection speed. By clicking-on the bandwidth connection field within the information and control console the user/subscriber will be re-directed to the service provisioning page to change the bandwidth to accommodate a higher or lower connection speed. The

start/stop button may also be implemented in this information and control console.

The information and control console is not limited to supplying information related to the user/subscriber's billing and service plans. It is also possible to configure the information and control console to include information that is customized to the user/subscriber or the location/site from which the user is remotely located. For example, the user may be located at a hotel for the purpose of attending a specific convention or conference either in the hotel or within the immediate vicinity of the hotel. The gateway interface may have "learned" this information about the user/subscriber through an initial log-on profile inquiry or the gateway administer may have inputted this information into a database. The gateway interface can store profile information within the user-specific AAA database or it can store and retrieve data from external databases. The gateway interface can be configured to recognize these profiles and to customize the information and control console accordingly. In the hotel scenario, the information and control console may include a link for convention or conference services offered by the hotel.

In another example of location specific information and control console data, the user subscriber may be remotely accessing the gateway interface while located in a specific airport terminal. The gateway interface will be configured so that it is capable of providing ready access to information related to that specific airport terminal, i.e. information pertaining to the current flights scheduled to depart and arrive that terminal, the retail services offered in that specific terminal, etc. In this manner, the information and control console may include a link for terminal specific flight information and/or terminal specific retail services available to the user/subscriber.

Customization of the information comprising the information and control console is not limited to the gateway administrator or the network operator. The user/subscriber may also be able to customize the information that is provided in the information and control console. The user/subscriber customization may be accomplished either directly by the user configuring the information and control console manually or indirectly from the gateway interface configuring the information and control console in response to data found in the user-specific profile. In the manual embodiment the user/subscribe may be asked to choose which information or type of information they would like supplied in the pop-up for that specific network session. For instance, the user may require an alarm clock counter to insure an appointment is met or the user may require periodical updates of a specific stock quote. The information that a user customizes for the information and control console may be network session specific, may be associated with the duration of a gateway subscription or may be stored in a user/subscriber profile for an indefinite period of time. The gateway interface's ability to communicate with numerous user databases provides the basis for storing user specific profiles for extended periods of time.

FIG. **7** illustrates an information and control console **110** that includes bandwidth up **112** selections for uploading data, bandwidth down **114** selections for downloading data, various internet links **116**, **118** and **120** and a user-specific link **122**. The user is able to modify bandwidths on-the-fly by selecting appropriate upload and download selections that meet the desired need of the user. For instance, if the user desires to download a data intensive file it may be desirable to increase the bandwidth and, thus, speed up the download process. Once the file has been downloaded the user may then select a more moderate bandwidth, typically at a lower billing rate. The example holds true for the upload of data. If the user desires to send a data intensive file it may be desirable to increase the bandwidth at which data is sent. The information and control console of this example also comprises a link to an Internet search engine **116**, an Internet auction site **118** and an Internet merchant **120**. These links provide the gateway administrator the capability to advertise to the user/subscribe other Internet sites. The user-specific link **122** provides the user/subscriber with linking capabilities to either information that the user has specifically demanded (e.g. stock quotes, news updates, etc.) or information that the user has shown an interest in (i.e. information learned by querying the user or through logging the Internet sites visited by the user).

FIG. **8** shows a flow diagram of a method for providing a network user with an information and control console that incorporates data in accordance with an embodiment of the present invention. At step **200**, the user establishes network access through a gateway interface that is in communication with the user's host and desired network. The gateway interface is capable of providing seamless network access without the need to reconfigure the host prior to network access. Communication between the user's host and the gateway interface can be accomplished though a conventional telephone/modem connection, a digital subscriber line (DSL), cable hook-up, wireless communication or any other suitable communication technique. Establishing access to the desired network will typically involve an authorization and authentication process and in some instances choosing a desired billing scheme and service level as offered by the gateway administrator or network operator. Once the user has established the network service connection and a tunnel has been opened to facilitate an open communication line between the user's host and the network, the gateway interface, at optional step **210**, communicates with various databases to assemble user-specific data. These databases may be internal databases located within the gateway interface or external databases located within the infrastructure of the composite network. The user-specific data that the gateway interface assembles may comprise billing scheme related data, service level data, user profile data, remote-site related data or any other data that is related to the user or the location from which the user is located during the networking session.

At step **220**, the gateway interface creates pop-up control packets that have attribute data related to the information that will be conveyed in the information and control console. These packets are typically written to accommodate standard Internet Protocol (IP). At step **230**, the packets are sent to the user's host and at step **240** an information and control console is generated on the monitor of the user's host that includes predefined information. In many instances, the information that is provided for in the pop-up control window will be user-specific information conveyed from a network user profile or directly input by the user/subscriber. As previously discussed the information provided in the information and control console may be links to advertising information, links to marketing information, network monitoring information or any other predefined information.

Many modifications and other embodiments of the invention will come to mind to one skilled in the art to which this invention pertains having the benefit of the teachings presented in the foregoing descriptions and the associated drawings. Therefore, it is to be understood that the invention is not to be limited to the specific embodiments disclosed and that modifications and other embodiments are intended

to be included within the scope of the appended claims. Although specific terms are employed herein, they are used in a generic and descriptive sense only and not for purposes of limitation.

That which is claimed:

1. A method for communicating to a host computer information during an existing networking session, the method comprising:

establishing, via a gateway interface, a network session between a host computer and a computer network;

creating, during the established network session, information and control console packets;

sending the information and control console packets to the host computer repeatedly throughout the network session; and

generating, during the established network session, one or more information and control console on a monitor of the host computer,

wherein the method provides a user an ability to re-configure the network session during the established network session by input to the information and control console.

2. The method of claim **1**, further comprising communicating, during the established network session, with databases in communication with the gateway interface to determine user-specific data that is used in creating information and control console packets.

3. The method of claim **2**, wherein the user-specific data comprises data related to a physical location of the host.

4. The method of claim **2**, wherein the user-specific data comprises data related to a profile of the user.

5. The method of claim **4**, further comprising querying the user and constructing the profile of the user based upon responses from the user to the query.

6. The method of claim **4**, further comprising logging networks, services and sites accessed by the user and constructing the profile of the user based upon the logged data.

7. The method of claim **2**, wherein creating, during the established network session, information and control console packets further comprises creating information and control packets at the gateway interface that reflect the user-specific data.

8. The method of claim **2**, wherein generating, in response to receipt of the information and control console packets, one or more information and control consoles on a monitor of the host computer further comprises generating, in response to receipt of the information and control console packets, one or more information and control consoles on a monitor of the host computer that comprises user-specific information.

9. The method of claim **8**, wherein the user-specific information includes a link to another available network.

10. The method of claim **8**, wherein the user-specific information includes a link to user-tailored marketing information.

11. The method of claim **8**, wherein the user-specific information includes a link to user-tailored advertising information.

12. The method of claim **8**, wherein the user-specific information includes a link to a gateway administrator survey.

13. The method of claim **1**, wherein generating, in response to receipt of the information and control console packets, one or more information and control consoles on a monitor of the host computer further comprises generating an information and control console on the monitor of the host computer that comprises generating, in response to receipt of the information and control console packets, one or more information and control consoles on a monitor of the host that comprises a link to another available network.

14. The method of claim **1**, wherein generating, in response to receipt of the information and control console packets, one or more information and control consoles on a monitor of the host computer further comprises generating, in response to receipt of the information and control console packets, one or more information and control consoles on a monitor of the host computer that comprises a link to marketing information.

15. The method of claim **1**, wherein generating, in response to receipt of the information and control console packets, one or more information and control consoles on a monitor of the host computer further comprises generating, in response to receipt of the information and control console packets, one or more information and control consoles on a monitor of the host computer that comprises a link to advertising information.

16. The method of claim **1**, wherein generating, in response to receipt of the information and control console packets, one or more information and control consoles on a monitor of the host computer further comprises generating, in response to receipt of the information and control console packets, one or more information and control consoles on a monitor of the host computer that comprises a link to a gateway administrator survey.

17. The method of claim **1**, wherein generating, in response to receipt of the information and control console packets, one or more information and control consoles on a monitor of the host computer further comprises generating, in response to receipt of the information and control console packets, one or more information and control consoles on a monitor of the host computer that comprises network monitoring information.

18. The method of claim **17**, wherein the network monitoring information includes at least one type of network monitoring information selected from the group consisting of user billing structure, user level of service, current network connection speed, quantity of data transferred, current charges accrued, elapsed time of network session, current time of day billing zone, current day of week billing zone, or current network status.

19. The method of claim **1**, further comprising sending information and control console monitor heartbeats from the host computer to the gateway interface following the generation of the information and control console, wherein the sending of information and control console monitor heartbeats occurs at predetermined intervals to notify the gateway interface that the information and control console monitor remains active.

20. The method of claim **19**, further comprising re-sending information and control console packets to the host computer in response to the gateway interface failing to receive information and control console monitor heartbeats after a predetermined period of time.

21. A method for dynamically changing user billing structure during an ongoing network session, the method comprising:

establishing, via a gateway interface, a network session between a host computer and a computer network;

creating, during the established network session, network monitoring information and control console packets that include information relating to the user-billing structure;

sending the network monitoring information and control console packets to the host repeatedly throughout the network session; and

generating, during the established network session, one or more network monitoring information and control consoles on a monitor of the host computer that provide a user an ability to change network session billing sure during the established network session.

22. The method of claim **21**, further comprising accepting, at the gateway interface, user responses to network monitoring information provided in the network monitoring information and control console to change the user-billing structure.

23. The method of claim **21**, wherein creating, during the established network session, network monitoring information and control console packets at the gateway interface network that include information relating to the user-billing structure further comprises creating, during the established network session, network monitoring information and control console packets at the gateway interface network information that includes information relating to at least one type of user-billing structure information selected from the group consisting of connection speed, quantity of data transmitted, time of day billing zones, time of week billing zones, or duration of network session.

24. The method of claim **21**, further comprising sending information and control console monitor heartbeats from the host computer to the gateway interface following the generation of the information and control console, wherein the sending of information and control console monitor heartbeats occurs at predetermined intervals to notify the gateway interface that the information and control console monitor remains active.

25. The method of claim **21**, further comprising re-sending information and control console packets to the host computer in response to the gateway interface failing to receive information and control console monitor heartbeats after a predetermined period of time.

26. A method for dynamically changing user level of service during an ongoing network session, the method comprising:

establishing, via a gateway interface, a network session between a host computer and a computer network;

creating, during the established network session, network monitoring information and control console packets that include information relating to the user level of service;

sending the network monitoring information and control console packets to the host periodically throughout the network session; and

generating, during the established network session, one or more network monitoring information and control consoles on a monitor of the host computer that provide a user an ability to change network session level of service during the established network session.

27. The method of claim **26**, further comprising accepting, at the gateway interface, user responses to network monitoring information provided in the network monitoring information and control console to change the user level of service.

28. The method of claim **26**, wherein creating, during the established network session, network monitoring information and control console packets at the gateway interface that include information relating to the user level of service further comprises creating, during the established network session, network monitoring information and control console packets at the gateway interface that includes information related to connection speeds.

29. A program storage device readable by a machine, tangibly embodying a program of instructions executable by the machine to perform steps for communication to a network user information during an ongoing networking session, the program of instructions comprising the steps of:

establishing, via a gateway interface, a network session between a host computer and a computer network;

creating, during the established network session, information and control console packets;

sending the information and control console packets to the host periodically throughout the network session; and

generating, during the established network session, one or more information and control consoles on a monitor of the host,

wherein the instructions provide a user an ability to re-configure the network session during the established network session by input to the information and control console.

30. The program storage device of claim **29**, further comprising communicating, during the established network session, with databases in communication with the gateway interface to determine user-specific data that is used in creating information and control console packets.

31. The program storage device of claim **29**, wherein creating, during the established network session, information and control console packets further comprises creating information and control packets at the gateway interface that reflect the user-specific data.

32. The program storage device of claim **29**, wherein generating, in response to receipt of the information and control console packets, one or more information and control consoles on a monitor of the host computer further comprises generating, in response to receipt of the information and control console packets, one or more information and control consoles on a monitor of the host computer that comprises user-specific information.

33. A computer program product, comprising:

a computer usable medium having a computer readable program code embodied therein for causing information to be provided to a network host during an ongoing networking session, the computer readable program code comprising:

computer-readable program means for causing a host computer to establish, via a gateway interface, a network session between a host computer and a computer network;

computer-readable program means for causing a host computer to create, during the established network session, information and control console packets;

computer-readable program means for causing a host computer to send the information and control console packets to the host repeatedly throughout the network session; and

computer-readable program means for causing a host computer to generate, during the established network session, one or more information and control consoles on a monitor of the host,

wherein the computer-readable program provides a user an ability to re-configure the network session during the established network session by input to the information and control console.

34. The computer program product of claim **33**, further comprising computer-readable program means for causing a host computer to communicate, during the established network session, with databases in communication with the gateway interface to determine user-specific data that is used in creating information and control console packets.

35. The computer program product of claim **33**, wherein the computer-readable program means for causing a host computer to create, during the established network session, information and control console packets at the gateway interface further comprises the computer-readable program means for causing a host computer to create information and control packets at the gateway interface that reflect the user-specific data.

36. The computer program product of claim **33**, wherein the computer-readable program means for causing a host computer to generate, in response to receipt of the information and control console packets, one or more information and control consoles on a monitor of the host computer-readable program means for causing a host computer to generate, in response to receipt of the information and control console packets, one or more information and control consoles on a monitor of the host user-specific information.

* * * * *